Program Directory for
RACF Security Server for z/VM

function level 610

Program Number 5741-A07

for Use with
z/VM version 6 release 1

Document Date: October 2009

GI11-4325-00

Attention

Before using this information and the product it supports, be sure to read the general information under “Notices” on page 112.

This program directory, dated October 2009, applies to IBM® RACF® Security Server for z/VM®, function level 610, Program Number 5741-A07.

A form for reader's comments appears at the back of this publication. When you send information to IBM®, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Figures

1.0 Introduction

This program directory is intended for the system programmer responsible for program installation and maintenance of the RACF® (Resource Access Control Facility) Security Server for z/VM®. It contains information concerning the material and procedures associated with the installation of RACF. You should read all of this program directory before installing the program and then keep it for future reference.

The program directory contains the following sections:

- 2.0, “Program Materials” on page 3 identifies the basic and optional program materials and documentation for RACF.
- 3.0, “Program Support” on page 6 describes the IBM support available for RACF.
- 4.0, “Program and Service Level Information” on page 8 lists the APARs (program level) and PTFs (service level) incorporated into RACF.
- 5.0, “Installation Requirements and Considerations” on page 10 identifies the resources and considerations for installing and using RACF.
- 6.0, “Installation Instructions” on page 22 provides detailed installation instructions for RACF.
- 7.0, “Service Instructions” on page 71 provides detailed servicing instructions for RACF.
- Appendix A, “Applying an RSU for RACF” on page 89 provides detailed Recommended Service Upgrade instructions for RACF.
- Appendix B, “RACF Local Modifications - Examples” on page 97 provides examples for putting on local modifications to RACF.
- Appendix C, “Starting, Stopping, and Disabling RACF” on page 108 provides information on starting, stopping and disabling RACF on your system.

Before installing RACF, read section 3.1, “Preventive Service Planning” on page 6. This section tells you how to find any updates to the information and procedures in this program directory.

1.1 Program Description

RACF Security Server for z/VM is a product that works together with the existing system features of VM to provide improved data security for an installation. To help an installation meet its unique security objectives, RACF provides:

- Protection of installation-defined resources

- Flexible control of access to protected resources
- The ability to store information for other products
- A choice of centralized or decentralized control profiles
- An ISPF panel interface and a command interface
- Transparency to end users
- Exits for installation-written routines.

For a more detailed description of RACF see *z/VM: RACF Security Server General User's Guide*. For a list of the books in the RACF library see section 2.3.2, "Base Program Publications" on page 4.

2.0 Program Materials

An IBM program is identified by a program number. The program number for RACF Security Server for z/VM, function level 610 is 5741-A07.

The program announcement material describes the features supported by RACF. Ask your IBM marketing representative for this information if you have not already received a copy.

The following sections identify:

- Basic and optional program materials available with this program
- Publications useful during installation.

2.1 Basic Machine-Readable Material

RACF Security Server for z/VM is distributed pre-installed as part of the z/VM System deliverable. Therefore, there are no basic machine readable materials.

RACF Security Server for z/VM is a priced feature, so it is installed disabled. **If you want to enable and use RACF then you MUST order the RACF Security Server for z/VM, function level 610, to obtain a license for it.** Refer to the z/VM version 6 release 1 announcement letter for information on ordering z/VM and its features, including RACF.

2.2 Optional Machine-Readable Material

There are no optional machine-readable materials for RACF.

2.3 Program Publications

The following sections identify the publications for RACF.

2.3.1 Basic Program Publications

One copy of the following is included when you order the basic materials for RACF.

Figure 1. Basic Material: Unlicensed Publications

Publication Title	Form Number
RACF Security Server for z/VM Program Directory	GI11-4325

2.3.2 Base Program Publications

Figure 2 identifies the program publications available for RACF.

Figure 2. Program Publications: New Editions

Publication Title	Form Number
z/VM: RACF Security Server Command Language Reference	SC24-6213
z/VM: RACF Security Server Security Administrator's Guide	SC24-6218
z/VM: RACF Security Server System Programmer's Guide	SC24-6219
z/VM: RACF Security Server Auditor's Guide	SC24-6212
z/VM: RACF Security Server General User's Guide	SC24-6215
z/VM: RACF Security Server Macros and Interfaces	SC24-6216
z/VM: RACF Security Server Messages and Codes	GC24-6217
z/VM: RACF Security Server Diagnosis Guide	GC24-6214

2.3.3 Softcopy Publications

The RACF publications are supplied softcopy as part of the *IBM Online Library: z/VM Collection on DVD* in Adobe® Portable Document Format (PDF) and in BookManager® format. One copy of the *IBM Online Library: z/VM Collection on DVD* is included when you order the basic materials for z/VM. RACF publications, except the Program Directory, are also available in the z/VM Information Center web site site:

http://publib.boulder.ibm.com/infocenter/zvm/v6r1/index.jsp

In addition, the RACF softcopy publications, including this Program Directory, are available in Adobe Portable Document Format from the z/VM internet library home page on the World Wide Web; the URL for this home page is:

www.ibm.com/servers/eserver/zseries/zvm

All the publications and collection kits can be ordered separately for a fee using the specific publication number through the IBM Publication Center at:

www.ibm.com/shop/publications/order

The Publications Center is a world wide central repository for IBM product publications and marketing material. Furthermore, a large number of publications are available online in various file formats (e.g. Adobe PDF), which can currently be downloaded free of charge.

2.4 Program Source Materials

No program source materials or viewable program listings are provided for RACF.

2.5 Publications Useful During Installation and Service

The publications listed in Figure 3 may be useful during the installation of RACF. To order copies, contact your IBM representative.

Figure 3. Publications Useful During Installation / Service on z/VM version 6

Publication Title	Form Number
z/VM: VMSES/E Introduction and Reference	GC24-6243
z/VM: Service Guide	GC24-6232
z/VM: CP Planning and Administration	SC24-6178
z/VM: CMS Commands and Utilities Reference	SC24-6166
z/VM: CMS File Pool Planning, Administration, and Operation	SC24-6167
z/VM: Other Components Messages and Codes	GC24-6207
z/VM: CMS and REXX/VM Messages and Codes	GC24-6161
z/VM: CP Messages and Codes	GC24-6177
z/VM: Running Guest Operating Systems	SC24-6228
z/VM: System Operation	SC24-6233

3.0 Program Support

This section describes the IBM support available for RACF.

3.1 Preventive Service Planning

Before installing RACF, check with your IBM Support Center or use IBMLink™ (ServiceLink) to see whether there is additional Preventive Service Planning (PSP) information. To obtain this information, specify the following UPGRADE and SUBSET values:

Figure 4. PSP Upgrade and Subset ID

	Retain		
COMPID	**Release**	**Upgrade**	**Subset**
576700201	610	RACFVM610	RACF610
576700201	610	RACFVM610	yynnRSU

Note: RSU-BY-LVL information can be obtained from the VM service RSU web site at:

www.ibm.com/eserver/zseries/zvm/service/rsu

3.2 Statement of Support Procedures

Note: With the RACF Security Server for z/VM feature that comes pre-installed on z/VM version 6, you are entitled to support under the basic warranty for z/VM version 6. Also, note that the Software Subscription and Support for the RACF Security Server for z/VM is *automatically* added to your order - this provides zSeries zSeries® service to which you are likely accustomed. If you do not want the Software Subscription and Support for RACF then you must take specific action to decline it when ordering.

Report any difficulties you have using the RACF product to your IBM Support Center. If an APAR is required, the Support Center will provide the address to which any needed documentation can be sent.

Figure 5 identifies the component ID (COMPID), Retain® Release and Field Engineering Service Number (FESN) for RACF.

Figure 5. Component IDs

	Retain		
COMPID	**Release**	**Component Name**	**FESN**
576700201	610	RACF FL610	6700201

4.0 Program and Service Level Information

This section identifies the program and any relevant service levels of RACF. The program level refers to the APAR fixes incorporated into the program. The service level refers to the PTFs shipped with this product. Information about the cumulative service tape is also provided.

4.1 Program Level Information

The following APAR fixes against RACF FL540 have been incorporated into this release:

VM64429 VM64557 VM64568 VM64581 VM64618
VM64627 VM64634

4.2 Service Level Information

Check the RACFVM610 PSP bucket for any additional PTFs that should be installed or any additional install information. This can be accomplished by checking with the IBM Support Center or using IBMLink (ServiceLink).

4.3 Cumulative Service

Cumulative service for RACF, function level 610, is available through a periodic Recommended Service Upgrade (RSU). The RSU is used to provide service updates for multiple z/VM components and features, including RACF, and is often referred to as a *stacked* RSU.

The z/VM V6 stacked RSU, which would include RACF, can be obtained by ordering PTF UM97610.

Check the PSP bucket upgrade RACFVM610 subset *yynn*RSU (where *yynn* is the RSU service level) for the latest RSU level for RACF. For the list of PTF's included on the RSU, refer to the RSU-BY-LVL information obtained from the VM service RSU web site at url:

www.ibm.com/eserver/zseries/zvm/service/rsu

4.4 How to Determine Your RSU Service Level

The service contained on each RSU constitutes a new service level. Use this service level when ordering corrective service. The service level is updated in the system inventory when the RSU is installed.

If you use the automated service procedures to install service then use the following command to query the current RSU service level of RACF.

service racf status

The output from this command is similar to the following console log. The VMFSRV1225I message indicates the RSU service level: 0901

```
VMFSRV2760I SERVICE processing started
VMFSRV1225I RACF (6VMRAC10%RACF) status:
VMFSRV1225I    Service Level     RSU-0901
VMFSRV1225I    Production Level  RSU-0901
VMFSRV2760I SERVICE processing completed successfully
```

Note: You can query the status of an APAR or PTF by using the SERVICE command above and placing the APAR or PTF number after the STATUS operand.

Or, you can use the following command anytime to query the RSU service level of RACF.

vmfsim query vm sysrecs tdata :ppf *compname* **:stat**

Use **RACF** if installed on minidisks or **RACFSFS** if installed in shared file system directories

The output from this command is similar to the following console log. The last part of the status line indicates the RSU service level: 0901

Note: You need to use the entry with the latest time stamp.

```
VMFSIP2408I RESULTS FOR
            TDATA :PPF RACF :STAT
:PPF 6VMRAC10 RACF
  :STAT RECEIVED.mm/dd/yy.hh:mm:ss.userid.RSU-0901
```

5.0 Installation Requirements and Considerations

The following sections identify the system requirements for installing and activating RACF Security Server for z/VM. These requirements apply whether you are installing RACF for the first time, or updating an existing system.

5.1 Hardware Requirements

RACF, function level 610, will operate on any processor supported by:

- z/VM version 6 release 1

On z/VM the minidisks for the RACF database (defined at virtual addresses 200 and 300) can reside on all DASD supported by z/VM version 6 release 1.

For the most current information on devices supported by z/VM version 6 release 1, refer to *z/VM General Information* manual. For more information on using FBA DASD devices, see 5.2.6, “Restrictions When Using FBA Devices” on page 17.

5.2 Program Considerations

The following sections list the programming considerations for installing RACF and activating its functions.

5.2.1 Operating System Requirements

RACF supports the following VM operating systems:

- z/VM version 6 release 1

5.2.2 Other Program Product Requirements

5.2.2.1 General

ISPF version 3 release 2 or later or ISPF/PDF is needed if you are planning on using the RACF ISPF panels.

Ensure that the ICKDSF level supports the DASD that you intend to use for the RACF databases. ICKDSF level 17 or higher comes with VM.

HLASM version 1 release 5 or higher is required if you intend to make changes to the RACF CP Parts or other RACF customizable parts, such as the RACF exits that are assemble files.

5.2.2.2 Dual Registration

If you have DirMaint™ installed, RACF provides dual registration panels so that you can add, change or delete information in the RACF database and the CP directory at the same time.

To use dual registration, you must have:

- ISPF version 3.2 or later

  - OR -
- DirMaint function level 610

5.2.3 Understanding RACF Interaction with CP

The RACF modules residing in the VM control program provide the interaction between RACF and VM. By convention, the module names begin with the prefix HCP. RACF modules residing in VM CP are:

HCPRPD
HCPRPF
HCPRPG
HCPRPI
HCPRPW
HCPRWA

RACF includes UPDATE files for HCPRWA, HCPRPD, HCPRPF, HCPRPG, HCPRPI, and HCPRPW with a filetype of RPIBASE0. During installation, the contents of these RACF UPDATE files replace the contents of the corresponding VM/CP ASSEMBLE files.

Note: An update file for HCPRWAC is also provided. This part is the Common Criteria compliant version of HCPRWA. If you intend to run a Common Criteria complaint configuration, see the *z/VM: Secure Configuration Guide* publication for more information.

For information on steps you need to perform to ensure that the CP part of RACF is installed properly, refer to 6.11, “Task 9. Install the CP Part of RACF” on page 46.

5.2.4 When the RACF Service Machine Is Uninitialized or Unresponsive

When the RACF service machine is uninitialized or unresponsive, no users are allowed to log on to the system, except for the following:

Any RACF service machine

The primary system operator or any of the defined alternate system operators, if there is no system operator currently logged on.

The userid currently logged on as system operator when the HERE operand is used on the LOGON command.

For these user IDs, the request is deferred to CP which checks the password supplied by the user against the password in the user's entry in the CP directory.

Note: By coding LOGONBY directory statements for the system operator user IDs or for RACF service machines, you still allow the use of LOGON BY for these user IDs when the RACF service machine is experiencing problems. This could be useful for recovery purposes.

5.2.5 Sharing a RACF Database

A RACF database can be shared with another operating system, either z/OS® or VM. In general a RACF database can be shared with a system that has another level of RACF installed. A RACF database residing on FBA DASD cannot be shared. See *z/VM: RACF Security Server System Programmer's Guide* for more information on sharing a RACF database.

Attention: Databases shared with z/OS

If the RACF database is to be shared with a z/OS system, it is recommended that the appropriate PTF for z/OS APAR OA22588 is applied and IRRMIN00 PARM=UPDATE run on z/OS.

Consider the following points if your installation plans to share the RACF database between two or more systems:

- System design in terms of DASD mapping
- Resource and load balancing
- Recovery and restart
- Operational control of the multi-processor environment
- Programming considerations for user resource protection
- Data integrity

During installation, if the database is not being shared, RACF issues a warning message:

```
CSTERP001W - Warning: Device xxx was configured as shared;
                      now configured as non-shared.
```

If you are not sharing a database you can ignore the message. If you are sharing a database and receive the message, you have not set up your database correctly.

RACF utilizes serialization, through reserve and release channel programs, to ensure the integrity of data stored in the RACF database between sharing RACF instances. Therefore, if you intend to share the RACF database, and the warning message CSTERP001W is issued during RACFVM initialization, **you must correct**

the situation to prevent database damage. The shared DASD environment must be properly defined to the z/VM Control Program in order for the corresponding serialization (for example, virtual and/or real reserve/release channel programs) to actually be reflected to the device on which the RACF database resides. Refer to the information in the following sections about sharing RACF databases.

When sharing databases, consider the following options when defining DASD:

- **If sharing between real systems (for example, two separate processors):**
  - Assign the entire volume using either the CP directory DEDICATE statement or full-pack MDISK statement.

    In deciding which statement to use be aware that the DEDICATE statement lets only one user access the disk drive through that **cuu** address, whereas the full-pack MDISK statement lets the disk be shared among virtual machines. A full-pack minidisk is a single minidisk allocated on an entire DASD volume encompassing all the primary (or addressable) tracks of the volume.

    If using an MDISK statement for the RACF database it must be setup up with MWV (for shared multiwrite mode). Virtual reserve/release must be enabled for any guest virtual machine reserve to be accepted, even if only one guest (such as RACFVM), is using the device. Virtual reserve/release allows reserve/release CCWs to be issued by the guest. Real reserve/release allows CCWs to reach the device. CP issues the reserve/release CCWs if both virtual reserve/release and real reserve/release are enabled.
  - Define the DASD as shareable to CP by coding it as shared in IOCP and coding the SHARED operand on the RDEVICE System Configuration file statement. Setting the SHARED operand to YES applies only to sharing full-pack minidisks between multiple real systems. (You can make the DASD sharable in between system IPLs by using the CP SET RDEVICE command with the SHARED YES operand.)
- **If sharing between virtual systems (for example, virtual and second-level guest systems):**

  This method is for sharing a minidisk between virtual systems on the same real system and not for sharing with another real system. z/VM CP simulates reserve/release if virtual reserve/release is enabled and real reserve/release is not. Virtual reserve/release allows reserve/release CCWs to be issued by the guest.
  - The MDISK Statement in the directory should specify an access mode of MWV (for shared multiwrite mode). The V suffix tells CP to support virtual reserve/release on I/O operations to the minidisk.
  - Specify that the DASD will not be shared with another operating system. The default setting of the SHARED operand on the RDEVICE System

Configuration file statement, which is SHARED NO, enables this configuration setting. A NO setting means this volume cannot be shared with an operating system running on another processor. (CP overhead is greater when you specify SHARED=YES as it directs CP to pass real reserve/release CCWS to the Real Device. It is not necessary for 'Virtual-Only' sharing).

- **If sharing between real and virtual systems (for example, two separate processors with at least one second-level guest):**

  This method of sharing DASD, concurrent virtual and real reserve/release, combines virtual reserve/release and real reserve/release. It allows DASD to be shared among multiple virtual machines and operating systems running on other processors.

  Concurrent virtual and real reserve/release involves the use of full-pack minidisks. The requirements are the same as when sharing between real systems except that DEDICATE is not an option. The DASD must be defined to CP as shareable and the MDISK directory statement must specify an an access mode of MWV.

  To summarize:

  – Use a full-pack minidisk (includes cylinder zero)

  – The MDISK directory statement must use the V statement (for example, MWV)

  – The System Configuration file requires RDEVICE statement with SHARED YES specified.

- If sharing with another system, ensure that the full pack minidisk on which the RACF database resides is **NOT** on a CSE formatted volume.
- MDC (minidisk caching) should be OFF for RACF database DASDs. The MDC feature is incompatible with DASD sharing in any form.
- z/VM CP and the directory program do not completely prevent you from defining minidisks that overlap. Overlap can defeat the integrity of link access modes and RESERVE/RELEASE serialization. Therefore, ensure that you validate the MDISK definitions for the RACF database volumes; overlaps must match completely.

5.2.5.1 Sharing RACF Databases with Another VM System

Attention - Important database information

Sharing RACF databases with RACF/VM FL530

It is essential that APAR VM64383 is applied to all RACF/VM FL530 systems that share the RACF database BEFORE running RACFCONV for RACF/VM FL610 or initializing RACF/VM FL610.

Note: After applying VM64383, you must restart your RACF FL530 Server. You can then continue with your migration or start sharing the RACF database.

VM64383 is also mandatory should you need to revert to RACF/VM FL530 and use the same database after initializing RACF/VM FL610. It is recommended that VM64383 be applied to your z/VM V5R3 system before starting the upgrade.

Failure to apply VM64383 to RACF/VM FL530 may result in the RACF database becoming unusable.

The VM restrictions and requirements for sharing DASD must be met. Information concerning VM requirements can be found in the VM library and should be reviewed for planning purposes:

- *z/VM System Operation*
- *z/VM CP Planning and Administration*
- *z/VM Running Guest Operating Systems.*

Decide where the RACF databases and libraries will be located, and whether there will be a single database or multiple databases. Information on splitting a database is in *z/VM: RACF Security Server System Programmer's Guide*. Make sure you review section 5.2.5, “Sharing a RACF Database” on page 12 for guidance, depending on the configuration that meets the needs of your installation and environment.

If you are sharing the RACF database exclusively with other RACF for z/VM systems, the templates must be at the same level on the sharing systems. Running the RACFCONV EXEC ensures that the templates are at the same level. See *z/VM: RACF Security Server System Programmer's Guide* for more information.

5.2.5.2 Sharing RACF Databases with a z/OS System

You can share a RACF database between a z/OS and a VM system. IBM strongly recommends that you review the *z/OS Security Server RACF System Programmer's Guide* for additional procedural and service recommendations that may be applicable to your installation; in particular sharing the RACF database

between z/OS and z/VM systems. In addition, the following items must be considered:

- **RACF databases during installation**

  The CP directory entry for the RACF service machine must be set up to refer to the z/OS volumes where the RACF databases are located. These volumes must be accessible by the VM system that is to share them. If the z/OS system is in a different host CPU (rather than a second level guest), the databases cannot be on VM minidisks. Attach or dedicate the volumes to the RACF service machine.

  You **must not** run the installation steps to format, allocate and initialize the RACF databases. You must allocate and reformat the RACF databases from z/OS.

  You must also system-generate the database as a shared device from the z/OS system that you are sharing the database with. For information about how to system-generate a device (the database) as shared in z/OS, refer to

  — *z/OS: HCD User's Guide*

  The RACF database names on the z/OS system will probably be different from those for VM. If this is the case, the RACF database names in ICHRDSNT ASSEMBLE must be changed to match the RACF database names used in the z/OS system. See *z/VM: RACF Security Server System Programmer's Guide* for more information.

- **RACF utilities and RACF Database templates**

  If you are running comparable levels of RACF on your VM and z/OS systems, it is recommended that you run the utilities from the z/OS system. However, if you are not running the same level of RACF on your VM and z/OS systems, you **must** run the RACF utilities from the system with the higher level of RACF.

  Attention: Databases shared with z/OS

  If the RACF database is to be shared with a z/OS system, it is recommended that the appropriate PTF for z/OS APAR OA22588 is applied and IRRMIN00 PARM=UPDATE run on z/OS.

  The RACF database templates supplied with RACF Security Server for z/VM FL610 are equivalent with those defined with the z/OS RACF V1.10 and any level of z/OS RACF with APAR OA22588 applied. Therefore, if you are sharing a RACF database with z/OS RACF V1.10 (or higher) or any z/OS RACF level with APAR OA22588 applied, it is not necessary to update the RACF database templates as the fields used by RACF Security Server for z/VM FL610 are already present in the shared RACF database.

  If you are sharing with a z/OS RACF V1.9 or lower system without APAR OA22588 then you need to run RACFCONV from RACF Security Server for

z/VM FL610 to update the RACF database templates. This is not a recommended sharing configuration.

5.2.6 Restrictions When Using FBA Devices

RACF supports the use of FBA devices, with the following restrictions:

- The minidisks defined at virtual addresses 200 and 300 for the RACF service machine must be 3370, 9332, 9335, 9336 or SCSI disks (which appear as 9336-20 DASD or SCSI FCP LUNs).

  For the most current information on FBA DASD devices supported by z/VM, refer to *z/VM: General Information* manual.
- RACF databases *cannot* be shared on FBA device types.
- The primary RACF database must have SYSRACF as the DDNAME in its FILEDEF statement. The backup RACF database must have RACFBKUP as the DDNAME in its FILEDEF statement.
- The number of RACF databases is limited to one primary and one backup.
- If the RACF database resides on an FBA DASD device, the multiple RACF service machines capability cannot be used.

5.2.7 Dynamic Parse Initialization

On VM, dynamic parse is started automatically by the RACF service machine during its initialization sequence. Refer to *z/VM: RACF Security Server System Programmer's Guide* for more information about dynamic parse.

5.2.8 RACF in conjunction with System Migration

If you use the migration procedure documented in the *z/VM: Guide for Automated Installation and Service* to migrate RACF from a z/VM V5.2, z/VM V5.3, or z/VM V5.4 system to z/VM V6.1, the customizable files will be migrated to z/VM V6.1, where possible. If the customizable files have been changed on the new level of RACF and you have made changes to them on your z/VM version 5 system, you will be told to rework your changes.

The RACF database disks will not be migrated.

5.2.9 VMSES/E Program Installation and Service Considerations

This section describes items that should be considered before you install or service RACF.

- VMSES/E is required to install and service this product.
- If multiple users install and maintain licensed products on your system, there may be a problem getting the necessary access to MAINT's 51D disk. If you find that there is contention for write access to the 51D disk, you can eliminate

it by converting the Software Inventory from minidisk to shared file system (SFS). See *VMSES/E Introduction and Reference* , section 'Changing the Software Inventory to an SFS Directory', for information on how to make this change.

- RACF can be serviced using user ID 6VMRAC10 or MAINT, if using automated service procedures. If you modify any user ID, minidisk address and SFS directory names you need to create a PPF override.

  Note - z/VM Automated Service Procedure

  If you modify any of the IBM-supplied default user IDs, minidisk addresses, or SFS directory names associated with RACF and you plan on using the z/VM automated service procedure (the **SERVICE** and **PUT2PROD** commands) to service your z/VM system, then you must create a PPF override for the **SERVP2P $PPF** file.

  You must also use the **VMFUPDAT** command to update the VM SYSSUF Software Inventory file, so that your PPF override for SERVP2P is used for automated service processing. For more information about PPF overrides, see the *VMSES/E Introduction and Reference*.

- RSU deliverables will be supplied as necessary. Service between RSUs can be obtained through CORrective service.

5.3 DASD Storage and User ID Requirements

Figure 6 lists the user IDs and minidisks that are used to install and service RACF.

Important Installation Notes:

- User ID(s) and minidisks are listed here so that you can get an idea of the resources that are needed. They are already defined and allocated on the z/VM System deliverable, as RACF is pre-installed.
- Figure 6 shows minimum space allocations. Depending on the requirements of your system, you might have to increase these sizes.

Figure 6 (Page 1 of 3). DASD Storage Requirements for Target Minidisks

Minidisk Owner (user ID)	Default Address	Storage in Cylinders		FB-512 Blocks	SFS 4K Blocks	Usage
		DASD	CYLS			Default SFS Directory Name
6VMRAC10	2B2	3390	85	122400	15300	Contains all the base code shipped with RACF **VMSYS:6VMRAC10.RACF.OBJECT**

See the notes following the table.

Figure 6 (Page 2 of 3). DASD Storage Requirements for Target Minidisks

Minidisk Owner (user ID)	Default Address	Storage in Cylinders		FB-512 Blocks	SFS 4K Blocks	Usage
		DASD	CYLS			Default SFS Directory Name
6VMRAC10	2C2	3390	9	12960	1620	Contains customization files. This disk can also be used for local modifications. **VMSYS:6VMRAC10.RACF.SAMPLE**
6VMRAC10	2D2	3390	70	100800	12600	Contains serviced files **VMSYS:6VMRAC10.RACF.DELTA**
6VMRAC10	2A6	3390	9	12960	1620	Contains AUX files and software inventory tables that represent the test service level of RACF **VMSYS:6VMRAC10.RACF.APPLYALT**
6VMRAC10	2A2	3390	9	12960	1620	Contains AUX files and software inventory tables that represent the service level of RACF that is currently in production. **VMSYS:6VMRAC10.RACF.APPLYPROD**
6VMRAC10	29E	3390	2	2880	NOSFS	Test general user disk. Code on this disk is copied to a production disk (for example MAINT 19E), so the production disk also requires this amount of free space.
6VMRAC10	590	3390	38	54720	NOSFS	Test CST/CMS system build disk.
6VMRAC10	505	3390	41	59040	NOSFS	Test server code build disk.
6VMRAC10	599	3390	31	44640	NOSFS	RACF ISPF Panels
6VMRAC10	191	3390	25+	36000+	NOSFS	6VMRAC10 user ID's 191 minidisk. See note 4 on page 21 for additional storage requirements.
RACFVM	490	3390	38	54720	NOSFS	Production CST/CMS system build disk.
RACFVM	305	3390	68	97920	NOSFS	Production server code build disk.
RACFVM	200	3390	17	24800	NOSFS	RACFVM primary database.
RACFVM	300	3390	17	24800	NOSFS	RACFVM backup database.
RACFVM	301	3390	7	10080	NOSFS	Primary SMF recording minidisk (5*)
RACFVM	302	3390	7	10080	NOSFS	Secondary SMF recording minidisk (5*)
RACFVM	191	3390	9	12960	NOSFS	RACFVM user ID's 191 minidisk

See the notes following the table.

Figure 6 (Page 3 of 3). DASD Storage Requirements for Target Minidisks

Minidisk Owner (user ID)	Default Address	Storage in Cylinders		FB-512 Blocks	SFS 4K Blocks	Usage
		DASD	CYLS			Default SFS Directory Name
RACFSMF	191	3390	10+	14400+	NOSFS	RACFSMF user ID's 191 minidisk See note 5 on page 21 for additional storage requirements.
RACFSMF	192	3390	10+	14400+	NOSFS	RACFSMF user ID's 192 minidisk See note 5 on page 21 for additional storage requirements.
AUTOLOG1	191	3390	5	7200	NOSFS	AUTOLOG1 user ID's 191 minidisk
AUTOLOG2	191	3390	5	7200	NOSFS	AUTOLOG2 user ID's 191 minidisk
RACMAINT	191	3390	9	12960	NOSFS	Backup RACFVM user ID's 191 minidisk.
IBMUSER	191	3390	1	____	____	IBMUSER user ID's 191 minidisk
SYSADMIN	191	3390	1	____	____	Optional. Security administrator's 191 minidisk. Not required if you are using an existing user ID for the security administrator.

See the notes following the table.

Notes:

1. Cylinder values defined in this table are based on a 4K block size. FB-512 block and SFS values are derived from the 3390 cylinder values in this table. The FBA blocks are listed as 512-byte blocks but should be CMS-formatted at 1K size. At least 32760 4K blocks are needed for SFS install.
2. Primary and backup minidisks should be on separate physical packs so that physical damage to one pack does not affect both primary and backup minidisks. If possible, the minidisks should also be on separate control units. For example, RACFVM's 191, 305, and 490 disks should not be on the same physical volumes as 6VMRAC10's 191, 29E, 505, and 590 disks, and if possible they should be on separate control units. Also, the RACFVM 200 and 300 database disks should be on separate physical packs and separate control units.
3. RACF supplies required virtual addresses and labels for the RACF databases; **you must not change them**. The label for the primary database is `RACF` at virtual address 200; the label for the backup database is `RACFBK` at virtual address 300.

   Do not place any of these minidisks on cylinder 0 in the CP directory. When the RACDSF EXEC executes, it could destroy the volume identifier on the pack.

Note: RACF and RACFBK are the default labels for the RACF databases. You can choose other non-duplicate labels.

4. On the 6VMRAC10 191 disk, plan on one additional megabyte of storage for each 10 000 commands created by the RPIDIRCT EXEC. (If you run RPIDIRCT from another user ID, plan on the same amount of storage for that ID.)
5. The size of the SMF recording minidisks should be governed by the amount of audit data recorded and the number of SECLABELS being audited.
6. If you are allocating the minidisks that RACFVM owns on 3390 DASD that has been configured in 3380 track-compatibility mode, you should use the minidisk size allocations listed in the 3380 CYLS column.
7. Refer to section 5.2.6, “Restrictions When Using FBA Devices” on page 17 for FBA restrictions.
8. NOSFS means this disk cannot be a shared file system directory.
9. The 6VMRAC10 590 disk and the RACFVM 490 disk must be the same DASD type and size.

6.0 Installation Instructions

Do you have a License for RACF Security Server for z/VM?

RACF Security Server for z/VM is pre-installed on z/VM version 6 using VMSES/E, in a DISABLED state. **If and only if**, you have a license for RACF Security Server for z/VM proceed with the installation to enable it for use.

This chapter describes the installation methods and the step-by-step procedures to install and activate RACF.

The step-by-step procedures are in two-column format. The steps to be performed are in bold large numbers. Commands for these steps are on the left hand side of the page in bold print. Additional information for a command might exist to the right of the command.

Each step of the installation instructions must be followed. Do not skip any step unless directed to do so.

Throughout these instructions, the use of IBM-supplied default minidisk addresses and user IDs is assumed. If you use different user IDs, minidisk addresses, or SFS directories to install RACF, adapt these instructions as needed for your environment.

Note!

The sample console output presented throughout these instructions was produced on a z/VM version 6 release 1 system.

6.1 Overview of the VMSES/E Installation Process

The following is a brief description of the main steps to complete the installation of RACF. (RACF was pre-installed, using VMSES/E, on the z/VM System deliverable.)

- Allocate resources

  Information for review on the user IDs associated with RACF. Also other important information on sharing the RACF database.

- Set RACF to the ENABLED state

  Use the VMSES/E SERVICE command to set RACF enabled so it can run.

- Perform post-installation tasks

Information about file tailoring and initial activation of the program is presented in 6.4, “Task 2. Convert the Database Templates” on page 28 through 6.20, “Task 18. Set Up the RACF ISPF Panels (Optional)” on page 58.

- Place RACF files into production

  Once the product files have been tailored and the operation of RACF is satisfactory, copy the product files from the test BUILD disk(s) to the production BUILD disk(s).

For a complete description of all VMSES/E installation options refer to *VMSES/E Introduction and Reference*.

6.2 Overview of the RACF Installation Steps

This overview describes the steps needed to complete the installation of RACF, function level 610.

Attention - RACF/VM FL530 Customers

It is essential that APAR VM64383 is applied to all RACF/VM FL530 systems prior to migrating to RACF/VM FL610.

Note: If you were an Early Support Program (ESP) customer for z/VM V5.3 and ran RACFCONV on the ESP code level of RACF FL530, you must run RACFCONV on the GA code level of RACF FL530 before proceeding with RACF FL610 initialization or applying the PTF for APAR VM64383.

After applying VM64383, you must restart your RACF FL530 Server. You can then continue with your migration or start sharing the RACF database.

In a shared database environment APAR VM64383 must be applied to all RACF/VM FL530 systems sharing the RACF database BEFORE running RACFCONV for RACF/VM FL610 or initializing RACF/VM FL610.

In a non-shared environment APAR VM64383 is mandatory should you need to revert to RACF/VM FL530 using the same database after initializing RACF/VM FL610.

Failure to apply VM64383 to RACF/VM FL530 may result in the RACF database becoming unusable.

Use the following checklist to track the installation steps for RACF as you complete them.

__ Task 1. Review information about resources for RACF, especially if you plan on sharing the RACF databases. Refer to 6.3, “Task 1. Review Resources for Installing RACF” on page 25.

__ Task 2. Skip this step, unless you are sharing or migrating an existing RACF database, as you may have to convert the database templates. Refer to 6.4, “Task 2. Convert the Database Templates” on page 28.

__ Task 3. Create an RPIDIRCT SYSUT1 file of RACF commands. Refer to 6.5, “ Task 3. Prepare to Update RACF with Existing CP Directory Data” on page 30.

__ Task 4. (*Optional*) Customize the RACFSMF user ID. Refer to 6.6, “Task 4. Customize the Processing of SMF Records (Optional)” on page 33.

__ Task 5. (*Optional*) Change the message routing table. Refer to 6.7, “Task 5. Change the Message Routing Table (Optional)” on page 36.

__ Task 6. (*Optional*) Add the ICHDEX01 Exit to Select Password Protection Algorithm. Refer to 6.8, “Task 6. Add the ICHDEX01 Exit to select Password Protection Algorithm” on page 39.

__ Task 7. (*Optional*) Delete or replace the ICHRCX02 Exit. Refer to 6.9, “Task 7. Delete or Replace the ICHRCX02 Exit (optional)” on page 40.

__ Task 8. (*Optional*) Customize RACF within CP. Refer to 6.10, “Task 8. Customize RACF Within CP (Optional)” on page 41.

__ Task 9. Enable and Install the CP part of RACF for VM. Refer to 6.11, “Task 9. Install the CP Part of RACF” on page 46.

__ Task 10. (*Customers sharing RACF databases*) Change RACF database names. Refer to 6.12, “Task 10. Change RACF Database Names If Sharing with z/OS System” on page 47.

__ Task 11. IPL the CP system with RACF. Refer to 6.13, “Task 11. IPL the CP System with RACF” on page 48.

__ Task 12. Initialize or update the RACF database. Refer to 6.14, “Task 12. Update the RACF Database with Existing CP Directory Information” on page 50.

__ Task 13. (*Optional*) Create the global access table. Refer to 6.15, “Task 13. Create the Global Access Table (Optional)” on page 55.

__ Task 14. (*Optional*) Set RACF options. Refer to 6.16, “Task 14. Set RACF Options (Optional)” on page 55.

__ Task 15. (*Optional*) Determine audit and control options for VM events. Refer to 6.17, “Task 15. Determine Audit and Control Options for VM Events (Optional)” on page 56.

__ Task 16. (*Optional*) Split the RACF database. Refer to 6.18, “Task 16. Split the RACF Database (Optional, Performance-Related)” on page 57.

__ Task 17. (*Optional*) Set up dual registration. Refer to 6.19, “Task 17. Set Up Dual Registration If DirMaint Is Installed (Optional)” on page 57.

__ Task 18. (*Optional*) Install the RACF ISPF panels. Refer to 6.20, “Task 18. Set Up the RACF ISPF Panels (Optional)” on page 58.

__ Task 19. Place RACF into production. Refer to 6.21, “Task 19. Place RACF Into Production” on page 67.

6.3 Task 1. Review Resources for Installing RACF

Procedural Note

Customers doing new installs and not sharing existing RACF databases should review the information in 6.3.1, “General RACF User ID Information” of this step and then skip to 6.5, “ Task 3. Prepare to Update RACF with Existing CP Directory Data” on page 30.

Customers doing new installs and sharing existing RACF databases should review the information in section 6.3.1, “General RACF User ID Information” and perform section 6.3.2, “Sharing a RACF Database Information” on page 27 of this step and then should skip to 6.4, “Task 2. Convert the Database Templates” on page 28.

This is a good time to consider Recovery Procedures should RACF become unresponsive. In particular, you can set up user IDs in the CP directory which are able to LOGON when RACF is unresponsive. See 5.2.4, “When the RACF Service Machine Is Uninitialized or Unresponsive” on page 11 for more information.

6.3.1 General RACF User ID Information

The planning information in the 6VMRAC10 PLANINFO file was used to create the 6VMRAC10, RACFVM, RACFSMF, RACMAINT, IBMUSER, AUTOLOG1, AUTOLOG2 and security administrator, SYSADMIN, user IDs supplied in the CP USER DIRECT file as supplied on the z/VM System deliverable.

The following is general information about the set up of the different RACF user ID directories:

- The RACMAINT user ID is used:
  - During installation as the RACF installation verification service machine
  - As a RACF service machine to test applied service

  This user ID can also be used as a backup RACF service machine to the RACFVM user ID, if that user ID becomes unusable. RACMAINT links to the test build disks that the 6VMRAC10 user ID owns.

- To facilitate the recovery procedure, allow RACFVM and RACMAINT all privilege classes except F. Do *not* specify class F, because you will want to have I/O errors reported, and specifying class F inhibits the reporting of I/O errors. The minimum required classes are B and G. Specifying class B allows RACFVM and RACMAINT to enter MSGNOH commands. Always specify the same minimum and maximum storage sizes on the USER statement for the RACFVM and RACMAINT directory entries.
- The RACF service machines must run in XA mode. The default names for the RACF service machines are RACFVM and RACMAINT.
- The minimum virtual storage size for the RACF service machines must be 20MB.
- You should use the recommended IUCV message limit settings for the RACF service machines as follows:

  ```
  IUCV *RPI PRIORITY MSGLIMIT 100
  IUCV  ANY PRIORITY MSGLIMIT  50
  ```

  This limit protects your RACF service machines from being overdriven by CP, as when a networking machine goes into recovery, and potentially leading to over-commitment of virtual resources within the RACF server.
- RACF supplies required virtual addresses and labels for the RACF databases; **you must not change these**. The label for the primary database is `RACF` at virtual address 200; the label for the backup database is `RACFBK` at virtual address 300.
- An AUTOLOG1 user ID must be set up.
- You can elect to use an existing user ID for the security administrator. The default user ID, shipped on the z/VM System deliverable, is SYSADMIN.

The following is general information about the set up of different minidisks:

- The 6VMRAC10 590 disk has been recomped to allow room for the CMS nucleus shipped with RACF. (To *recomp* is to redefine the number of cylinders or blocks available to you on a disk.) The following figure shows what recomp amount was used for your DASD type.

Figure 7. CMS Recomp Amounts

Device Type	**Recomp (*xxxx*)**
3390	32
FBA	46500

The RACF CMS was generated on the 590 disk using the GENNUC command.

- The RACF database minidisks, RACFVM 200 and 300, have been formatted, allocated and initialized on the z/VM System deliverable using the RACF commands RACDSF or RACFBK, RACALLOC and RACINITD.

Procedural Note

Customers doing new installs and not sharing existing RACF databases should continue with step 6.5, " Task 3. Prepare to Update RACF with Existing CP Directory Data" on page 30.

Customers sharing the RACF databases should continue with the next step.

6.3.2 Sharing a RACF Database Information

Attention - Important database information

Sharing RACF databases with RACF/VM FL530

It is essential that APAR VM64383 is applied to all RACF/VM FL530 systems that share the RACF database BEFORE running RACFCONV for RACF/VM FL610 or initializing RACF/VM FL610.

Note: After applying VM64383, you must restart your RACF FL530 Server. You can then continue with your migration or start sharing the RACF database.

VM64383 is also mandatory should you need to revert to RACF/VM FL530 and use the same database after initializing RACF/VM FL610. It is recommended that VM64383 be applied to your z/VM V5R3 system before starting the upgrade.

Failure to apply VM64383 to RACF/VM FL530 may result in the RACF database becoming unusable.

The MDISK statement for the 200 and 300 disks should specify `MW`, unless you are sharing the RACF database between different systems or multiple servers. If you are sharing the RACF database between different systems, see 5.2.5, "Sharing a RACF Database" on page 12. If you are sharing the RACF database between multiple servers, see *z/VM: RACF Security Server System Programmer's Guide*.

Attention

It is **very important** that you review the above information about sharing and set up the appropriate RACF CP user directory entries, etc., if you plan on sharing the RACF database.

Procedural Note

Customers doing new installs and sharing existing RACF databases or migrating existing RACF databases should continue with step 6.4, "Task 2. Convert the Database Templates" on page 28 after setting up the RACF databases for sharing.

Customers doing new installs and not sharing the RACF databases should continue with step 6.5, " Task 3. Prepare to Update RACF with Existing CP Directory Data" on page 30.

6.4 Task 2. Convert the Database Templates

Procedural Note

Customers doing new installs and sharing or migrating an existing RACF database should perform this step.

Customers doing new installs and not sharing the RACF database should skip to 6.5, " Task 3. Prepare to Update RACF with Existing CP Directory Data" on page 30.

If you were an Early Support Program (ESP) customer for z/VM V5.3 and ran RACFCONV on the ESP code level of RACF FL530, you must run RACFCONV on the GA code level of RACF FL530 before proceeding with RACF FL610 initialization or applying the PTF for APAR VM64383.

If you are migrating from z/VM V5.3 RACF FL530, or if you plan to share your z/VM V6.1 RACF FL610 database with z/VM V5.3 RACF FL530, you must apply the PTF for APAR VM64383 to your z/VM V5.3 system (and restart your RACF FL530 server) before attempting any migration or sharing.

The RACF database must have templates at the function level 610 for RACF to function properly. If you are migrating from a previous release of RACF to RACF FL610, you must run the RACFCONV EXEC to convert the existing database templates to the current release.

Be sure to run RACFCONV against each primary and backup database on your system.

Note: This is not a conversion to the restructured database format.

If you are sharing the RACF database, you must convert the templates from the system with the highest level of RACF. See sections 5.2.5.1, "Sharing RACF Databases with Another VM System" on page 14 and 5.2.5.2, "Sharing RACF

Databases with a z/OS System" on page 15 for information on highest levels of RACF.

To convert the database templates from a VM system use the following instructions. (To convert the database templates from a z/OS system, see *z/VM: RACF Security Server System Programmer's Guide*.)

1 Run RACFCONV EXEC to convert the templates.

link RACFVM 200 200 mr
racfconv

```
This exec is used to run the Racf utility IRRMIN00 to
convert existing Racf datasets for a new release of Racf.

Press ENTER to continue....
```

ENTER

```
Enter the device address to be converted
```

200

```
About to update templates in 'RACF.DATASET' at virtual address '200'
Do you wish to continue?

Enter YES or NO
```

yes

```
Processing begins
All output will be placed in the MIN00U OUTPUT file on the 'A' disk.
Program 'IRRMIN00' is being executed - Please wait -


Processing complete
Return code from 'IRRMIN00' = 0
Ready; T=0.07/0.10 11:41:46
```

link RACFVM 300 300 mr
racfconv

```
This exec is used to run the Racf utility IRRMIN00 to
convert existing Racf datasets for a new release of Racf.

Press ENTER to continue....
```

ENTER

```
Enter the device address to be converted
```

300

```
About to update templates in 'RACF.BACKUP' at virtual address '300'
Do you wish to continue?

Enter YES or NO
```

yes

```
Processing begins
All output will be placed in the MIN00U OUTPUT file on the 'A' disk.
Program 'IRRMIN00' is being executed - Please wait -


Processing complete
Return code from 'IRRMIN00' = 0
Ready; T=0.07/0.10 11:44:44
```

det 200
det 300

6.5 Task 3. Prepare to Update RACF with Existing CP Directory Data

Procedural Note

Customers doing new installs should perform this step.

Attention - Important database information

Using a RACF/VM FL610 database with RACF/VM FL530

It is essential that APAR VM64383 is applied to all RACF/VM FL530 systems that may use a RACF database initialized by RACF/VM FL610.

Note: After applying VM64383, you must restart your RACF FL530 Server. You can then continue with your migration or start sharing the RACF database.

VM64383 is also mandatory should you need to revert to RACF/VM FL530 and use the same database after initializing RACF/VM FL610. It is recommended that VM64383 be applied to your z/VM V5R3 system before starting the upgrade.

Failure to apply VM64383 to RACF/VM FL530 may result in the RACF database becoming unusable.

The RPIDIRCT EXEC helps you to migrate existing CP directory data to a RACF database. It scans the CP directory and translates directory statements into RACF commands. It places the RACF commands in an output file called RPIDIRCT SYSUT1. You can use this file to initialize new RACF databases if you are not planning on sharing an existing RACF database, or to modify an existing database if you are planning on sharing an existing RACF database.

Before you run RPIDIRCT, you might need to make some changes to the CP directory. After you run RPIDIRCT, you might need to make some changes to the RPIDIRCT SYSUT1 file.

For information on using RPIDIRCT see chapter "Preparing to Use RACF", section "Using RPIDIRCT to Prime the RACF Database from the CP Directory", in the *z/VM: RACF Security Server Security Administrator's Guide* (SC24-6218).

6.5.1 Run RPIDIRCT to Create the RPIDIRCT SYSUT1 File

The RPIDIRCT EXEC needs access to three minidisks:

- A minidisk with the CP directory
- A minidisk with the DirMaint cluster files (if applicable)
- A minidisk for the RACF command output generated by the RPIDIRCT EXEC

1 You should be logged on to the 6VMRAC10 user ID.

2 Link and access the disk that contains your CP directory file. (The default CP directory file name is USER DIRECT and it resides on MAINT's 2CC minidisk.)

Note: If you are currently running DirMaint then you need to issue the DIRM USER WITHPASS command and put the resulting file on MAINT's 191 A-disk and call it USER WITHPASS. This is the name of the file you want to use in the step that follows that has you issue the rpidirct command. Also you need to link MAINT's 191 disk instead of the 2CC disk.

3 If applicable, link and access the disk that contains DirMaint cluster files. By default the DirMaint cluster files reside on the DIRMAINT 1DF disk. You will need to know the READ password in order to link to this disk.

4 Ensure that the 6VMRAC10 191 disk has enough free space and that the user ID building the database (later in the installation) has access to the 6VMRAC10 191 disk.

5 Make sure the CP directory entries will not cause any problems. Refer to the section "General CP Directory Requirements" in the *z/VM: RACF Security Server Security Administrator's Guide* (SC24-6218).

6 Create the CMS file of RACF commands, RPIDIRCT SYSUT1. This file will be used by another step further on in the install process.

access 505 e
rpidirct *fn ft fm outmode*

Where *fn ft fm* is the name of your CP directory file (ie.USER DIRECT or USER WITHPASS) and *outmode* is the file mode where you want the created RPIDIRCT SYSUT1 file placed. The default for outmode is A.

Note: This step might take a while to run, and the output comes to the console. If you do not want to see the output then spool your console before you enter the command (so that you will be able to view any error messages) and type `HT` after the RPIDIRCT command starts.

7 Make any changes to the RPIDIRCT SYSUT1 file that your installation requires, as discussed in the *z/VM: RACF Security Server Security Administrator's Guide* (SC24-6218), section "Using RPIDIRCT to Prime the RACF Database from the CP Directory".

In order to use z/VM Automated Service

In order to use the z/VM automated service commands you need to give UACC of UPDATE for VMRDR to the MAINT user ID.

6.6 Task 4. Customize the Processing of SMF Records (Optional)

Procedural Note

This step is optional.

The RACFSMF user ID can be set up to automatically perform SMF switching and archiving tasks. RACF keeps track of unauthorized attempts to log on to the system by writing an SMF record to the SMF DATA file. An installation can optionally have RACF write SMF records for any authorized attempts and/or unauthorized attempts for the following activities:

- Attempts to access RACF-protected resources
- Attempts to enter RACF commands or certain CP commands and diagnose codes
- Attempts to modify profiles in the RACF database

A single-record file named SMF CONTROL exists on RACFVM's 191 disk. It identifies two SMF minidisks (301 as the primary minidisk, 302 as the secondary minidisk) that RACF uses to record audit information. RACF refers to this file to determine which disk to use first. When RACF fills that minidisk, RACF switches to the other SMF minidisk, updates the SMF CONTROL file to reflect the change, and autologs the RACFSMF user ID.

For detailed information on the RACFSMF user ID and the SMF CONTROL file, see *z/VM: RACF Security Server Auditor's Guide*.

6.6.1 Setting Up the RACFSMF PROFILE EXEC (Optional)

A sample profile exec for the RACFSMF user ID is provided on the 6VMRAC10 505 test build disk. The file SMFPROF EXEC can be copied to the RACFSMF user ID and renamed to PROFILE EXEC. Without changing any of the variables in the exec, RACFSMF will automatically perform SMF switching and archiving tasks. Your installation can change the default values.

The variables and their defaults are:

- *SMFDISK* gives the virtual address of the disk on which archived SMF DATA is to be copied. The default value is `192`.
- *SMFPCT* is the percentage to which the SMF archive disk fills. The default setting is `80`. If the SMF archive disk gets more than 80% full, a message is sent to a designated user ID.
- *SMFINFO* is the user ID that receives the disk full message. The default user ID is `OPERATOR`.

- *SMFFREQ* controls the frequency of SMF switching and archiving. Valid values are `DAILY`, `WEEKLY`, or `MONTHLY`. If you initialize *SMFFREQ* as `MONTHLY`, you should also initialize variable *SMFDAY* to a day of the week.

  If you chose `TUESDAY` and `MONTHLY`, for example, SMF switching and archiving takes place on the first Tuesday of each month.

  The default settings are `SMFFREQ=WEEKLY` and `SMFDAY=MONDAY`.

- *SMFSWTCH* indicates whether RACFSMF is to be autologged by RACFVM when the SMF disk is full or on a regular basis. The default is `YES` (archiving on a regular basis). If you want to use this exec only when the SMF disk is full, specify `SMFSWTCH NO`.

RACFSMF requires ALTER access to RACFVM's 301 and 302 disks, and requires READ access to RACFVM's 191 disk. The links to the 301 and 302 disks are performed during the RACFSMF autolog. IBM recommends that you define RACFSMF to a group with `TERMUACC(NONE)` so that no one can manually log on to RACFSMF.

When the SMF DATA files are copied to the 192 disk, they will always have a file name that reflects the Julian date on which switching took place, for example, SMF07122. If more than one file is archived on one day the *file type* will reflect the backup number (DATA, DATA0001, DATA0002, etc.).

RACFSMF is automatically logged off. The SMF records on the 192 disk are ready for processing by your installation. Refer to *z/VM: RACF Security Server Auditor's Guide* for more information on using SMF records.

1 Link and access RACFSMF's 191 disk.

```
link racfsmf 191 291 mr
access 291 m
```

2 Copy the sample PROFILE EXEC for the RACFSMF user ID.

copyfile smfprof exec *fm-505* **profile exec m (olddate replace**

Where *fm-505* is the current file mode of 6VMRAC10's 505 test build disk.

3 Make any required updates to the PROFILE EXEC.

4 Detach the RACFSMF disk.

```
det 291
```

6.6.2 Setting Up the SMF CONTROL File (Optional)

At initialization, RACF uses the SMF CONTROL file to determine on which of two minidisks to record SMF records. When RACF fills up the minidisk on which it began recording, it uses the SMF CONTROL file to determine the location of the alternate minidisk.

When it switches minidisks, RACFVM updates the CURRENT field in the SMF CONTROL file (on RACFVM's A-disk) to reflect the minidisk that it is now recording on.

If the default addresses, filemodes, and CPU IDs specified in the file shipped with RACF do not fit the needs of your installation, you can edit the SMF CONTROL file and change them.

Following is the default SMF control record contained in the SMF CONTROL file:

```
CURRENT 301 K PRIMARY 301 K SECONDARY 302 K 10000 VMSP CLOSE 001 SEVER NO 0 RACFSMF
```

In this record, the virtual addresses of the SMF minidisks are 301 and 302. The filemode is K, the default maximum buffer size for the SMF DATA file is 10000, and VMSP is the ID of the CPU where RACF generates the SMF records. CLOSE *nnn* specifies the number of audit records RACF buffers before they are written to the SMF file. You can specify 000-999; the default value is 001.

RACF limits the CPU ID to four characters. It is used as an identifier for SMF records and should not be confused with the larger CPU ID in VM systems.

The CLOSE 001 ensures that the audit requests processed by RACF are not buffered before being written to the SMF data file.

If you specify CLOSE 000, the file is not explicitly closed by RACF; CMS writes the audit records when the internal buffer is full. Note that if *nnn* is large, RACF can write more audit records per second, thereby improving system performance. However, more audit records could be lost during a system failure.

The SEVER keyword is initially set to NO. If the installation chooses to set SEVER to YES, RACF will sever the path between CP and RACF when the SMF disks are full, and RACF is unable to continue recording SMF records. Before setting SEVER to YES, installations should consider its effect on system availability.

The 0 is an internal flag used by RACF, and should not be altered by the user.

RACFSMF is the user ID that is autologged when the 301 or 302 minidisks are filled.

If you XEDIT the SMF CONTROL file, you must not alter the format of the control record: a single space must separate operands. In addition, the SMF CONTROL file must be a fixed block logical record length of 100.

If you change the SMF CONTROL file, you need to copy it to RACMAINT's 191 disk.

1 Link and access RACFSMF's 191 disk.

```
link racfsmf 191 291 mr
access 291 m
```

2 Copy the SMF CONTROL file.

```
link racfvm 191 391 mr
access 391 n
copyfile smf control n = = m (olddate replace
```

3 Make any required updates to the SMF CONTROL file on the 291 minidisk.

4 Copy the new SMF CONTROL file to the RACFVM and RACMAINT 191 A-disks.

```
link RACMAINT 191 491 mr
access 491 o
copyfile smf control m = = o (olddate replace
copyfile smf control m = = n (olddate replace
```

5 Detach the RACFSMF, RACFVM, and RACMAINT disks.

```
det 291
det 391
det 491
```

6.7 Task 5. Change the Message Routing Table (Optional)

Procedural Note

This step is optional.

RACF simulates OS multiple console support by using the VM MSG, WNG, SMSG, and MSGNOH commands. The simulation uses a routing table (CSTCONS) to send console messages to VM user IDs.

The CSTCONS routing table shown in Figure 8 is the table shipped with RACF and is called CSTCONS ASSEMBLE. It contains the following:

- The user IDs that receive the text of WTO/WTOR SVCs
- The commands (MSG, WNG, SMSG, or MSGNOH) used to send the text of the WTO/WTOR SVCs
- A list of the routing codes each user ID in the table should receive

```
CSTCONS  CSECT           MCS TABLE OF USER IDS
* ENTRY FORMAT:
*
* |-------------------------------------------------------------------|
* | ROUTCODES   |       TARGET USERID            |      MSG MODE      |
* |-------------------------------------------------------------------|
* 0             2                                10                  15
MCSR1    EQU   X'80'          MASTER CONSOLE
MCSR2    EQU   X'40'          MASTER CONSOLE INFORMATIONAL
MCSR3    EQU   X'20'          TAPE POOL
MCSR4    EQU   X'10'          DIRECT ACCESS POOL
MCSR5    EQU   X'08'          TAPE LIBRARY
MCSR6    EQU   X'04'          DISK LIBRARY
MCSR7    EQU   X'02'          UNIT RECORD POOL
MCSR8    EQU   X'01'          TELEPROCESSING POOL
MCSR9    EQU   X'80'          SYSTEM SECURITY
MCSR10   EQU   X'40'          SYSTEM/ERROR MAINTENANCE
MCSR11   EQU   X'20'          PROGRAMMER INFO
MCSR12   EQU   X'10'          EMULATOR INFORMATION
MCSR13   EQU   X'08'          USER ROUTING
MCSR14   EQU   X'04'          USER ROUTING
MCSR15   EQU   X'02'          USER ROUTING
MCSR16   EQU   X'01'          AUTHORIZATION FOR SMSG TO RACF SERVER
*
FF       EQU   255
         SPACE 3
MASTRCON DC    AL1(FF),AL1(FF-MCSR9-MCSR11),CL8'*',CL6'MSGNOH'
SECCON   DC    X'00',AL1(MCSR9),CL8'OPERATOR',CL6'MSGNOH'
SEC2CON  DC    X'00',AL1(MCSR16),CL8'RACFSMF',CL6'MSGNOH'
END      DC    XL2'00'
         END
```

Figure 8. Example of CSTCONS Routing Table.

If your installation uses the CSTCONS routing table shipped with RACF, RACFVM all/localmodsages with all routing codes, except security routing codes (route code 9) that go to the OPERATOR, and “Write to Programmer” messages (route code 11) that are ignored.

If you want a user ID other than OPERATOR to receive the messages with security routing codes, replace OPERATOR with that user ID in the CSTCONS table. If you want another user ID (such as a system administrator), in addition to OPERATOR, to receive the messages with security routing codes, add that user ID to the CSTCONS table without deleting OPERATOR. You must add any additional user IDs to the table after the MASTRCON statement and before the END statement.

The SECCON statement identifies the OPERATOR in the CSTCONS table.

For example, if you want the user ID SYSDA to receive the messages with security routing codes, add the statement below after the SECCON statement and before the END statement.

```
THRDCON  DC  X‘00’, AL1(MCSR9), CL8‘SYSDA’, CL6‘MSGNOH’
```

This entry in the table causes the system to route security messages to SYSDA in addition to routing them to the operator.

Notes:

1. If a message is sent to a user who is not logged on when the message is sent, the message is forwarded to RACFVM. The user ID (in parentheses) of the user for whom the message was intended precedes the message.
2. IBM recommends placing the security administrator in the CSTCONS table so that the security administrator can receive security-relevant messages and respond to RACF prompts.

6.7.1 Updating the Message Routing Table

To update the message routing table, do a VMSES/E local modification to the CSTCONS ASSEMBLE and CSTCONS TEXT file.

Follow the steps documented in B.1, “Assemble Full Part Replacement - Example” on page 97 to perform the local modification to CSTCONS files. Use the following substitution values:

- For *fn* use **CSTCONS**
- For *nnnn* use **0001**
- For *blist* use **RPIBL505**
- For *memname* use **CSTCONS**

At the end of the procedure your modified copy of CSTCONS ASSEMBLE and CSTCONS TEXT will be on 6VMRAC10's 505 test build disk. It will be copied to RACFVM's 305 production build disk in the copy to production step later on.

6.8 Task 6. Add the ICHDEX01 Exit to select Password Protection Algorithm

Procedural Note

Customers who want to use DES encryption as the password protection algorithm can bypass this task, as it is now the default. If you would like to use hashing, please perform this task.

Another way to customize RACF is to add an ICHDEX01 exit.

6.8.1 The ICHDEX01 Exit (Hashing or DES Encryption)

To provide password protection, early releases of RACF included a routine for masking passwords stored on the RACF database. Later, RACF offered the option of improved password protection using the Data Encryption Standard (DES) algorithm to encrypt passwords. However, some installations already had installation-written exit routines in place that expect masking, not encryption. To remain compatible with those installations, RACF provides a sample installation exit which activates the masking algorithm. This sample exit (ICHDEX01) always returns a return code of 4 which in turn causes RACF to use the masking algorithm for passwords.

Note!

RACF prior to RACF FL610 was shipped with this exit enabled and if DES encryption was desired then the exit had to be deleted from RACFLPA LOADLIB.

If you choose to use the masking algorithm instead of the DES algorithm, you must add the sample exit to RACFLPA LOADLIB, and re-IPL RACFVM. This same change should be made to the service machine's 505 disk.

Note: If you choose to use the DES algorithm, you must use it on all systems that share the RACF database.

For more information, refer to *z/VM: RACF Security Server System Programmer's Guide* and *z/VM: RACF Security Server Security Administrator's Guide*.

6.8.1.1 Adding ICHDEX01

To add ICHDEX01 TEXT, follow the instructions in B.3, "Local Modification to Full Part Replacement Text Files and Possible Build List Update" on page 100 using the following substitution values:

- For *fn* use **ICHDEX01**
- For *blist* use **RPIBLLPA**. You will need to do the steps to get the highest level of a part and the remove object step for the build list.
- For *nnnn* use **0002**
- For *libname* use **RACFLPA** and for *libftype* use **LOADLIB**. You need to copy the library into production.

Notes:

1. If you want use a local mod rather than the sample ICHDEX01 TEXT create the ASSEMBLE file and follow the appropriate steps in B.3, "Local Modification to Full Part Replacement Text Files and Possible Build List Update" on page 100.
2. Note that you will uncomment the following section in the RPIBLLPA build list:

```
*:OBJNAME. ICHDEX01 LEPARMS RENT REUS LET NCAL XREF DCBS SIZE 100K,80K
*:BLDREQ. RPIBLOBJ.ICHDEX01
*:OPTIONS. CONCAT SYSLIB RACFOBJ
*:OPTIONS. INCLUDE RACFOBJ(ICHDEX01)
*:OPTIONS. ENTRY ICHDEX01
*:EOBJNAME.
```

3. You should not do the last step, which is to re-ipl the RACF service machine.

6.9 Task 7. Delete or Replace the ICHRCX02 Exit (optional)

Procedural Note

This step is optional.

Another way to customize RACF is to delete or replace the ICHRCX02 exit.

6.9.1 The ICHRCX02 Exit

The RACROUTE REQUEST=AUTH (also known as RACHECK) postprocessing exit, ICHRCX02, is shipped with the RACF for VM product. This exit allows an alternate user to access resources that a user can access, but which the alternate user cannot normally access. The requests are re-driven using the ACEE of the service machine when the request is for a resource in the VMNODE, VMRDR or VMMDISK class. It can be used, for example, to allow users to access a restricted

compiler only when submitting a batch job to a specified batch machine. If you do not want this postprocessing exit, delete it.

6.9.1.1 Modifying ICHRCX02

If you want to modify ICHRCX02 ASSEMBLE and TEXT, follow the instructions in B.4, "Local Modification to Full Part Assemble and Text Files and Possible Build List Update" on page 103, using the following substitution values:

- For *fn* use **ICHRCX02**
- For *nnnn* use **0002**

Note: You will not be adding or deleting anything to a build list, so you can skip those steps.

6.9.1.2 Deleting ICHRCX02

If you are deleting ICHRCX02, you need to local modify the RPIBLLPA build list to reflect this. Follow the instructions in B.4, "Local Modification to Full Part Assemble and Text Files and Possible Build List Update" on page 103, using the following substitution values:

- For *fn* use **ICHRCX02**
- For *blist* use **RPIBLLPA**

Note: You need to do the VMFSETUP step, and then start with the step to get the highest level of the build list. You should not do the last step, which is to re-ipl the RACF service machine.

6.10 Task 8. Customize RACF Within CP (Optional)

Procedural Note

This step is optional.

There are several RACF options that you can customize within the CP modules, including the following:

- SYSSEC parameters
- Issuance of RACF messages
- Public minidisks
- The requirement for passwords for a RACF command session
- User IDs for RACF service machines
- Multiple RACF service machines
- The value of the POSIX constant NGROUPS_MAX

6.10.1 Setting the CP Disposition for Access Requests (Optional)

Until you have RACF installed to your satisfaction, you might want CP to continue to make access decisions for some of your resources; for example, nodes, minidisks, and commands. (For the protected commands in VM, refer to *z/VM: RACF Security Server Security Administrator's Guide*)

The SYSSEC macro establishes a relationship between RACF's response to an access request and the final disposition of that request.

The defaults for SYSSEC parameters are shown in Figure 9.

You should be careful about changing the "CP Disposition" on minidisk relationships. *Do not change it to "Disallow Access."* Resources are not defined when IBMUSER logs on after the initial IPL. If you disallow access, IBMUSER is not granted access to CMS minidisks that IBMUSER requires to initialize the RACF database.

See *z/VM: RACF Security Server Macros and Interfaces* for a description of the SYSSEC macro.

RACF Response	CP Disposition
Access Permitted	Allow Access
Resource Undefined	Defer to CP
Access Denied	Disallow Access
Access denied, but warning mode is set for resource	Defer to CP

Figure 9. Initial Relationships between Access Decisions Made by RACF and Final Disposition by CP

In the figure, if a user attempts to LINK to a minidisk that has not been defined to RACF, the request is deferred to VM. VM permits the user to link if the user has supplied a valid LINK password.

To update or change the SYSSEC macro invocation parameters in HCPRWA, put a local modification on to HCPRWA RPIBASE0. See 6.10.8, "Performing a Local Modification to HCPxxx" on page 45 for the steps to local mod HCPRWA.

6.10.2 Suppressing Issuance of RACF Messages (Optional)

Options in the SYSSEC macro allow you to suppress the issuance of RACF-defined error messages which result from unsuccessful authorization checks by RACF (messages issued by the VM operating system are still displayed). Messages can be suppressed for any combination of the resource classes VMMDISK, VMRDR, VMNODE, VMCMD and VMLAN.

The default is for messages to be displayed. To change the settings, you need to change the SYSSEC parameters in HCPRWA.

Refer to *z/VM: RACF Security Server Macros and Interfaces* for a description of the SYSSEC macro.

To update or change the SYSSEC macro invocation parameters in HCPRWA, put a local modification on to HCPRWA RPIBASE0. See 6.10.8, “Performing a Local Modification to HCPxxx” on page 45 for the steps to local mod HCPRWA.

6.10.3 Defining Public Minidisks (Optional)

Within the CP modules, you can define public minidisks (minidisks for public access). Defining public minidisks can improve performance because read access to them is automatically granted without calling the RACF service machine. To define a minidisk as public, use the GLBLDSK macro to define the minidisk in the global minidisk table. For information on the global minidisk table and how to identify minidisks that can be considered public minidisks, refer to *z/VM: RACF Security Server System Programmer's Guide* and *z/VM: RACF Security Server Macros and Interfaces*. For information on the GLBLDSK macro, see *z/VM: RACF Security Server Macros and Interfaces*.

To update or change the GLBLDSK macro invocation parameters in HCPRWA, put a local modification on to HCPRWA RPIBASE0. See 6.10.8, “Performing a Local Modification to HCPxxx” on page 45 for the steps to local mod HCPRWA.

6.10.4 Requiring Passwords for RACF Command Sessions (Optional)

RACF does not require that users enter their passwords to establish RACF command sessions. However, if your installation wants its users to enter passwords for RACF command sessions, you must change the assembler statement in HCPRPD from:

```
&NPWD SETB 1
```

to

```
&NPWD SETB 0
```

To update or change HCPRPD, put a local modification on to HCPRPD RPIBASE0. See 6.10.8, “Performing a Local Modification to HCPxxx” on page 45 for the steps to local mod HCPRPD.

For information on RACF command sessions, see *z/VM: RACF Security Server Command Language Reference*. Note that a logon password is always required, even if a password is not required for RACF command sessions.

6.10.5 Changing User IDs for RACF Service Machines (Optional)

If you are using user IDs other than RACFVM and RACMAINT for the RACF service machines, you need to update the RACSERV macro statements in HCPRWA. See *z/VM: RACF Security Server Macros and Interfaces* for details on the RACSERV macro.

To update the RACSERV macro statements in HCPRWA, put a local modification on to HCPRWA RPIBASE0. See 6.10.8, "Performing a Local Modification to HCPxxx" on page 45 for the steps to local mod HCPRWA.

Note: The RACSERV statements must immediately follow the HCPRWATB entry definition label in HCPRWA.

6.10.6 Defining Multiple RACF Service Machines (Optional)

It is strongly recommended that you install the RACF product and determine the overall system performance characteristics before you install multiple RACF service machines. See *z/VM: RACF Security Server System Programmer's Guide* for information on the benefits of using multiple RACF service machines, how to determine if you need more than a single RACF service machine, and the procedure for installing multiple service machines.

If you plan to install multiple RACF service machines, IBM recommends that you make changes to the RACSERV invocations in HCPRWA as part of RACF installation, leaving the other multiple service machine installation tasks for a later time. This allows you to avoid a CP nucleus regeneration at that time.

To update the RACSERV macro statements in HCPRWA, put a local modification on to HCPRWA RPIBASE0. See 6.10.8, "Performing a Local Modification to HCPxxx" on page 45 for the steps to local mod HCPRWA.

Note: The RACSERV statements must immediately follow the HCPRWATB entry definition label in HCPRWA.

6.10.7 Specifying the Value of the POSIX Constant NGROUPS_MAX (Optional)

The POSIX constant NGROUPS_MAX defines the number of supplemental GIDs that are associated with a POSIX process for authorization. You specify the value of the NGROUPS_MAX constant on the ICHNGMAX macro. See *z/VM: RACF Security Server Macros and Interfaces* for a description of the ICHNGMAX macro. If a valid value for the NGROUPS_MAX constant is specified on the ICHNGMAX macro at initialization, RACF support for OpenExtensions for VM is activated.

We do not recommend that you specify a value for NGROUPS_MAX at install time unless you are sure that you want RACF support for OpenExtensions for VM activated at install time. *z/VM: RACF Security Server Security Administrator's*

Guide contains a complete description of the steps required to activate the RACF support for OpenExtensions for VM. If you specify a value for NGROUPS_MAX at install time, make sure that you also perform the steps documented in *z/VM: RACF Security Server Security Administrator's Guide*.

6.10.8 Performing a Local Modification to HCPxxx

To update or change the HCP*xxx* files you need to put a local modification on to HCP*xxx* RPIBASE0, where *xxx* can be RWA, RPD, RPI, RPW, RPF, or RPG.

Follow the steps below to perform the local modification to HCP*xxx* RPIBASE0. Use the following substitution values:

- For *fn* use **HCP***xxx*, where *xxx* is RWA, RPD, RPI, RPW, RPF or RPG.
- For *ft* use **RPIBASE0**.
- For *nnnn* use **0001**.

1 Make sure you are logged on to the 6VMRAC10 user ID.

2 Establish the 6VMRAC10's minidisk access order.

vmfsetup SERVP2P {RACF | RACFSFS}

SERVP2P is a z/VM system supplied PPF file that overrides the 6VMRAC10 RACF PPF file. Use RACF if installing on minidisks or RACFSFS if installing on SFS directories.

3 Copy the file to the 2C2 (E-disk) using the local modification identifier and update the VVT table for the part or file.

vmfrepl *fn ft* **SERVP2P {RACF | RACFSFS} ($select logmod L***nnnn* **outmode localsam**

Note: *nnnn* is a user-defined number assigned to this fix, usually starting with 0001.

4 Make your local modification changes to the copy on the LOCALSAM 2C2 disk.

The modified HCP*xxx* RPIBASE0 files will be built on 6VMRAC10's 505 test build disks and then will be copied to the CP maintenance user ID's local modification disk in step 6.11, “Task 9. Install the CP Part of RACF” on page 46. It is in that step that your changes will be assembled and built into the CP nucleus.

6.11 Task 9. Install the CP Part of RACF

Procedural Note

All customers should perform this step.

The enablement of RACF is needed before RACF can be used.

The installation of the CP part of RACF, into the CP nucleus, is needed in order to run RACF.

Modules HCPRPI, HCPRPD, HCPRPF, HCPRPG, HCPRPW, and HCPRWA are placeholders in the VM control program and provide the interaction between RACF and VM. The RACF install replaces the contents of these VM/CP ASSEMBLE files.

Follow these steps to enable RACF and apply the RACF updates to CP:

1. Log on to the CP maintenance ID, MAINT (which is the default user ID).
2. Enable RACF, install the CP part of RACF and generate new CP nucleus.

service racf enable

   The new CP nucleus, with the RACF CP parts, was placed on the secondary parm disk (default disk address of CF2).

   For your information, a copy of the previous (or currently running) CPLOAD MODULE is still on the primary (CF1) and tertiary (CF3) parm disks as CPLOAD MODULE. It is also saved on the secondary parm disk as CPLOLD MODULE.

   Note: If you update the HCPMDLAT macro to add or modify the position of the RACF modules in the CP load list, you should **not** add these entries to an AUXRPI file. The preferred AUX file will prevent the VM updates from being included when the macro is built. See *z/VM: Service Guide* for instructions on updating the CP load list.

3. Review the message log ($VMFSRV $MSGLOG). If necessary, correct any problems before going on. For information about handling specific error messages, see *z/VM: System Messages and Codes,* or use on-line HELP.

vmfview service

6.12 Task 10. Change RACF Database Names If Sharing with z/OS System

Procedural Note

Follow the instructions in this section only if:

- You are doing a new install

  AND

- You are sharing your RACF databases with a z/OS system

  AND

- The RACF database names on the z/OS system are different than the default database names shipped with RACF

Otherwise, continue with 6.13, “Task 11. IPL the CP System with RACF” on page 48.

If the RACF database names on the z/OS system are different than those defaulted for VM, you need to change the RACF database names in the ICHRDSNT ASSEMBLE and ICHRDSNT TEXT files to match the z/OS system. These files reside on 6VMRAC10's 505 test build disk. See *z/VM: RACF Security Server System Programmer's Guide* for information on the ICHRDSNT files.

To change the ICHRDSNT ASSEMBLE and TEXT files you must perform a local modification against them. Follow the steps documented in B.1, “Assemble Full Part Replacement - Example” on page 97 to perform the local modification, using the following substitution values:

- For *fn* use **ICHRDSNT**.
- For *nnnn* use **0001**.
- For *blist* use **RPIBL505** and **RPIBLLNK**. (Do the VMFBLD twice, once for each buildlist.)
- For *memname* use **ICHRDSNT**.

At the end of the procedure your modified copies of ICHRDSNT ASSEMBLE, ICHRDSNT TEXT, and the RACFLINK LOADLIB (containing the new ICHRDSNT) will be on 6VMRAC10's 505 test build disk.

6.13 Task 11. IPL the CP System with RACF

Procedural Note

All customers should perform this step.

Attention - Important database information

Using a RACF/VM FL610 database with RACF/VM FL530

It is essential that APAR VM64383 is applied to all RACF/VM FL530 systems that may use a RACF database initialized by RACF/VM FL610.

Note: After applying VM64383, you must restart your RACF FL530 Server. You can then continue with your migration or start sharing the RACF database.

In a shared database environment APAR VM64383 must be applied to all RACF/VM FL530 systems sharing the RACF database BEFORE running RACFCONV for RACF/VM FL610 or initializing RACF/VM FL610.

In a non-shared environment APAR VM64383 is mandatory should you need to revert to RACF/VM FL530 using the same database after initializing RACF/VM FL610. It is recommended that VM64383 be applied before starting the upgrade.

Failure to apply VM64383 to RACF/VM FL530 may result in the RACF database becoming unusable.

In this task you will IPL your system with the NOAUTOLOG option. After the system IPL, XAUTOLOG the RACMAINT user ID, which will initialize RACF. At this time the CP nucleus built with RACF is on the secondary (CF2) parm disk.

If RACF cannot find the database name in the database name table (ICHRDSNT) during initialization, it might be for one of the following reasons:

- The database name specified in ICHRDSNT does not match the data set name on the database DASD volumes.
- The database name contains an asterisk (*).
- No FILEDEF exists for the RACF database.

In each instance, the system prompts the system operator for a RACF database name.

From the system operator's console, do **one** of the following:

Enter: `SEND RACMAINT 1RACF.DATASET`

replacing RACF.DATASET with your installation's RACF database name

OR

Enter: `SEND RACMAINT 1NONE`

Note: If you specify `SEND RACMAINT 1NONE`, RACF is not active for this IPL. This is not recommended, because most users will not be able to log on to the system. (Only RACF servers, or the primary system operator, will be able to log on using the directory password.)

1 Make sure you are logged onto MAINT or equivalent user ID in order to shutdown the system.

shutdown

2 IPL the system using the CF2 parm disk, as this is where the new CP nucleus was placed in 6.11, “Task 9. Install the CP Part of RACF” on page 46.

To IPL from the CF2 parm disk you need to use the loadparm parameter on the IPL command; which will display the Stand-Alone Program Loader panel.

You will need to know your console address. You can get this by doing a QUERY CONSOLE.

Note: The following instruction can be used if you are IPLing second level. If you are IPLing first level, see the appropriate processor operator's guide for the system console, for instructions.

IPL *rdev* **CLEAR LOADPARM** *cons*

rdev is the address of the real DASD device containing your system residence volume.

cons is the address of your console

3 Change the **EXTENT** field to a **2** and press the **PF10 key** to LOAD on the Stand Alone Program Loader screen. Following is an example of the screen with EXTENT field filled in with a 2.

```
STAND ALONE PROGRAM LOADER: z/VM VERSION 5 RELEASE 4.0

DEVICE NUMBER:  rdev        MINIDISK OFFSET:   00000000   EXTENT:  2

MODULE NAME:     CPLOAD     LOAD ORIGIN:       1000

--------------------------------IPL PARAMETERS--------------------------


-----------------------------------COMMENTS-----------------------------



------------------------------------------------------------------------


9= FILELIST  10= LOAD  11= TOGGLE EXTENT/OFFSET
```

4 IPL with **NOAUTOLOG**.

When you see the following on the console:

```
hh:mm:ss  Start ((Warm|Force|COLD|CLEAN) (DRain) (DIsable)  (NODIRect)
hh:mm:ss        (NOAUTOlog)) or (SHUTDOWN)
```

Reply with the following; along with any other parameters you need:

NOAUTOLOG

Answer any other replies the way you would for any other IPL of your VM system.

5 Once the system is IPLed you need to type in the following from the system operator's console.

XAUTOLOG RACMAINT

6 You can then disconnect from the operator and continue with the next task.

6.14 Task 12. Update the RACF Database with Existing CP Directory Information

Procedural Note

Customers doing new installs should perform this step.

If you are not sharing another system's existing RACF database you are creating a new RACF database, and you need to initialize your new RACF database with information that is in your CP directory.

If you are sharing another system's existing RACF database, then you need to update the shared RACF database with information that is in your CP directory.

The CP directory information that you need to update or migrate to the RACF database is contained in the RPIDIRCT SYSUT1 file, in the form of RACF commands. You created this file in 6.5, " Task 3. Prepare to Update RACF with Existing CP Directory Data" on page 30.

Procedural Note

If you are **not sharing** existing RACF databases with another system, continue with section 6.14.1, "Initialize the RACF Database (If You Are Not Sharing an Existing Database)."

If you **are sharing** existing RACF databases with another system, continue with section 6.14.2, "Update the RACF Database (If You Are Sharing an Existing Database)" on page 54.

6.14.1 Initialize the RACF Database (If You Are Not Sharing an Existing Database)

To initialize the RACF database, you need to:

- Log on to the IBMUSER user ID.
- Run RPIBLDDS to build the RACF database.
- Define the security administrator.

6.14.1.1 Logging On to the IBMUSER User ID

The first time you IPL your system with RACF active, RACF automatically initializes the RACF database with a set of basic profiles to help you achieve system security quickly. One of these is the IBMUSER user ID.

IBMUSER is connected to three group profiles named SYS1, VSAMDSET, and SYSCTLG. (VSAMDSET and SYSCTLG are subgroups of SYS1.)

This user ID gives you full authority, including the SPECIAL and OPERATIONS attributes, to use any of the RACF functions. Links in IBMUSER's CP directory entry (for the system 190 and system 19E disks) are not in the RACF database at this point. If you are deferring minidisk access decisions for undefined resources to CP, you can ignore the warning messages that RACF is generating.

For more information, refer to *z/VM: RACF Security Server Security Administrator's Guide*.

Note: If you specified the CP disposition for `Resource Undefined` to be "Disallow Access" (you are *not* deferring minidisk access decisions), CP does not allow IBMUSER to link to the CMS minidisks. If you did this by mistake, you must go back to 6.10.1, "Setting the CP Disposition for Access Requests (Optional)" on page 42. Correct any incorrect entries in HCPRWA. You will then have to regenerate the CP nucleus (see step 6.11, "Task 9. Install the CP Part of RACF" on page 46, using only the options $SELECT and NOCOPY on the VMFREPL command and then update the HCPxxx existing part on 6VMRAC10's 2C2 (localsam) disk) and then IPL (see step 6.13, "Task 11. IPL the CP System with RACF" on page 48).

1 Log on to the IBMUSER user ID. Enter a password of SYS1. You will be prompted to enter a new password.

Note: You cannot run RPIBLDDS from RACMAINT or RACFVM.

6.14.1.2 Building the RACF Database

1 Link and access 6VMRAC10's 505, 191, and 29e disks

```
link 6VMRAC10 505 305 rr
acc 305 c
link 6VMRAC10 191 192 rr
acc 192 b
link 6VMRAC10 29e 29e rr
acc 29e d
```

Need to have access to the RPIDIRCT SYSUT1 file (created by RPIDIRCT earlier in the install) and the RPIRAC MODULE.

2 Run RPIBLDDS

RPIBLDDS runs the commands contained in RPIDIRCT SYSUT1, the output file created by RPIDIRCT.

Depending on the size of the database you are building, the job might take a long time. You might want to split the RPIDIRCT file into smaller files, thereby breaking the task into several more manageable tasks. Each of the smaller files **must** have a FILETYPE of SYSUT1. You would then invoke RPIBLDDS with the filename of each smaller file supplied as a parameter. For example, you could split RPIDIRCT SYSUT1 into 2 files called RPIDIR1 SYSUT1 and RPIDIR2 SYSUT1. You would then invoke RPIBLDDS with the following commands: `RPIBLDDS RPIDIR1` and `RPIBLDDS RPIDIR2`.

rpibldds *fn*

Where *fn* is the name of the SYSUT1 file. The default *fn* is RPIDIRCT. Keep in mind that if you split the RPIDIRCT SYSUT1 file then you need to execute RPIBLDDS for each file.

6.14.1.3 Defining the Security Administrator and Maintenance User IDs.

In 6.3, “Task 1. Review Resources for Installing RACF” on page 25 the default user ID, SYSADMIN, was supplied on the z/VM System deliverable as the security administrator user ID. You must now change the RACF user profile to give the security administrator RACF “special” authority. (Do this while logged on to the IBMUSER user ID.)

1 Define the Security Administrator User ID

RAC ALTUSER *userid* **SPECIAL**

Where *userid* is the user ID of your security administrator. There is a default user ID, SYSADMIN, set up in the z/VM CP directory that you can use.

2 Define two Maintenance User IDs (needed in order to use the automated service procedure to install service to RACF)

RAC ALTUSER MAINT OPERATIONS
RAC ALTUSER BLDSEG OPERATIONS

MAINT is the default maintenance user ID that is used by the automated VMSES/E service commands.

3 Log off IBMUSER and log on to the security administrator user ID.

You are now ready to begin using this user ID for security administration.

4 Because IBMUSER is an IBM-defined user ID, it might be a target for unauthorized accesses to your system. To prevent further use of the IBMUSER user ID, we recommend that you revoke the user ID:

link 6VMRAC10 29e 29e rr
acc 29e d
RAC ALTUSER IBMUSER REVOKE

Note: The IBMUSER user ID cannot be deleted.

We also suggest that you remove the SPECIAL and OPERATIONS attributes from the IBMUSER user ID:

RAC ALTUSER IBMUSER NOOPERATIONS NOSPECIAL

Where to Next?

Continue with section 6.15, “Task 13. Create the Global Access Table (Optional)” on page 55.

6.14.2 Update the RACF Database (If You Are Sharing an Existing Database)

1 Make sure the RACMAINT service machine is active.

2 Log on to the security administrator ID or any user ID with SPECIAL authority.

Note: You cannot run RPIBLDDS from RACMAINT or RACFVM.

3 Link and access 6VMRAC10's 505, 191, and 29e disks.

```
detach 505
detach 305
link 6VMRAC10 505 305
acc 305 c
link 6VMRAC10 191 192
acc 192 b
link 6VMRAC10 29e 29e rr
acc 29e d
```

Need to have access to the RPIDIRCT SYSUT1 file (created by RPIDIRCT earlier in the install) and the RPIRAC MODULE.

4 Run RPIBLDDS.

RPIBLDDS runs the commands contained in RPIDIRCT SYSUT1, the output file created by RPIDIRCT.

Depending on the size of the database you are building, the job might take a long time. You might want to split the RPIDIRCT file into smaller files, thereby breaking the task into several more manageable tasks. Each of the smaller files **must** have a FILETYPE of SYSUT1. You would then invoke RPIBLDDS with the filename of each smaller file supplied as a parameter. For example, you could split RPIDIRCT SYSUT1 into 2 files called RPIDIR1 SYSUT1 and RPIDIR2 SYSUT1. You would then invoke RPIBLDDS with the following commands: `RPIBLDDS RPIDIR1` and `RPIBLDDS RPIDIR2`.

rpibldds *fn*

Where *fn* is the name of the SYSUT1 file. The default fn is RPIDIRCT. Keep in mind that if you split the RPIDIRCT SYSUT1 file then you need to execute RPIBLDDS for each file.

6.15 Task 13. Create the Global Access Table (Optional)

Procedural Note

This step is optional.

If you choose not to perform this step, skip to 6.16, “Task 14. Set RACF Options (Optional).”

You can create the global access table to define your global resources to RACF. See *z/VM: RACF Security Server Security Administrator's Guide* for information on creating and updating the global access table.

The global access table is not required, but it is recommended because it can improve performance. If you choose not to create the global access table at this time, the security administrator can create it at a later time.

6.16 Task 14. Set RACF Options (Optional)

Procedural Note

This step is optional but you need to make note of the information below about what needs to be set to use the VMSES/E automated service commands (SERVICE, PUT2PROD) as you are going to want to set those authorizations at some point.

If you choose not to perform this step, skip to 6.17, “Task 15. Determine Audit and Control Options for VM Events (Optional)” on page 56.

Use the SETROPTS command to set RACF options. See *z/VM: RACF Security Server Security Administrator's Guide* for information on the SETROPTS options and how to set them.

If you choose not to set RACF options at this time, the security administrator can set them at a later time.

NOTE

If you decide to wait to provide access authorization for general resource classes then you will see many RPIMGR031E (Resource xxxxx specified by link command not found) messages. This is okay as the resource will be linked. The command that provides access authorization for general resource classes is; where you would supply the name of the resource:

```
RAC SETROPTS CLASSACT(resource)
```

In order to use the automated service procedures to service RACF you have to provide access authorization for the following general resource classes:

```
RAC SETROPTS CLASSACT(VMMDISK)
RAC SETROPTS CLASSACT(VMRDR)
RAC SETROPTS CLASSACT(VMBATCH)
RAC SETROPTS CLASSACT(VMSEGMT)
```

If you are using SFS directories for any product's service disks then you will need to provide access authorization to the SFS (shared file system) general resource classes.

6.17 Task 15. Determine Audit and Control Options for VM Events (Optional)

Procedural Note

This step is optional.

If you choose not to perform this step, skip to 6.18, "Task 16. Split the RACF Database (Optional, Performance-Related)" on page 57.

When you install RACF on VM, by default the following VM events are protected by RACF:

- APPCPWVL
- COUPLE.G
- DIAG0A0
- DIAG0D4
- DIAG0E4
- DIAG088
- DIAG280
- DIAG290
- FOR.C
- FOR.G
- LINK

- MDISK
- RSTDSEG
- STORE.C
- TAG
- TRANSFER.D
- TRANSFER.G
- TRSOURCE

By default, no VM events are audited.

If you want to change these default control or audit settings, you must create a VMXEVENT profile and activate it using the SETEVENT command.

For information on controlling VM events, see *z/VM: RACF Security Server Security Administrator's Guide*. For information on auditing VM events, see *z/VM: RACF Security Server Auditor's Guide*.

6.18 Task 16. Split the RACF Database (Optional, Performance-Related)

Procedural Note

This step is optional.

If you choose not to perform this step, skip to 6.19, “Task 17. Set Up Dual Registration If DirMaint Is Installed (Optional).”

If all you need is one primary and one backup database, and you are satisfied with the default performance options, you can skip this step. If you plan to split your database, see *z/VM: RACF Security Server System Programmer's Guide* for information on splitting databases.

6.19 Task 17. Set Up Dual Registration If DirMaint Is Installed (Optional)

Procedural Note

This step is optional.

If you choose not to perform this step, skip to 6.20, “Task 18. Set Up the RACF ISPF Panels (Optional)” on page 58.

RACF can coexist with the VM Directory Maintenance (DirMaint) product installed. However, to avoid dual maintenance of password processing (and other RACF functions), you must do the following:

1. Use the DirMaint supplied sample file CONFIGRC SAMPDVH. You need to copy this file to the 6VMDIR10 11F disk as CONFIGRC DATADVH. Refer to the *Directory Maintenance Facility Tailoring and Administration Guide*, Chapter 3, "Tailoring the DIRMAINT Service Machine", Step 5. Select RACF-Specific Characteristics, for information about this file. For this to take effect, either IPL DirMaint or enter the DIRM RLDDATA command.
2. If you want to record DirMaint activity in RACF SMF records, enable the ESM_LOG_RECORDING_EXIT. To do this, remove the comment from the item ESM_LOG_RECORDING_EXIT in the CONFIGRC DATADVH file. For this to take effect, either IPL DirMaint or enter the DIRM RLDDATA command.
3. You must also authorize the DirMaint service machines DIRMAINT, DATAMOVE, and DIRMSAT to use the RACROUTE interface. For more information, see *Directory Maintenance Facility Tailoring and Administration Guide* and *z/VM: Security Server RACROUTE Macro Reference*.

For further information about using DirMaint with RACF see the information on external security manager considerations in *Directory Maintenance Facility Tailoring and Administration Guide*, Appendix A 'External Security Manager Considerations'.

6.20 Task 18. Set Up the RACF ISPF Panels (Optional)

Procedural Note

If you want to use the RACF ISPF panels, then you need to follow the steps in this section to set them up.

- If you have ISPF/PDF installed, continue with section 6.20.1, “Modify the ISPF Files For Use With PDF” on page 59.
- If you do not have ISPF/PDF installed, continue with section 6.20.2, “Modify the ISPF Files for use with non-PDF” on page 61.

Otherwise, if not using ISPF at all, skip to 6.21, “Task 19. Place RACF Into Production” on page 67.

6.20.1 Modify the ISPF Files For Use With PDF

Refer to *ISPF version 3 for VM Dialog Management Guide* (SC34-4221) for information about updating the ISPF panel libraries.

6.20.1.1 Step 1 - Modify the ISPF EXEC Filedefs

Figure 10 on page 60 shows an example of how you should modify the filedefs in your installation's ISPF EXEC if PDF is installed on your system. For your convenience, this example is included on the 6VMRAC10 599 test build disk in a file named ISPFRACF EXECSAMP.

```
/*                                                                  */
/* FILEDEFS FOR PANEL LIBRARIES                                     */
/*                                                                  */
'FILEDEF ISPPLIB DISK DUALPLIB MACLIB  * (PERM CONCAT'
'FILEDEF ISPPLIB DISK HRFPANL  MACLIB  * (PERM CONCAT'
'FILEDEF ISPPLIB DISK ISRNULL PANEL  * (PERM CONCAT'
'FILEDEF ISPPLIB DISK ISRPLIB MACLIB * (PERM CONCAT'
'FILEDEF ISPPLIB DISK ISPPLIB MACLIB * (PERM CONCAT'
/*                                                                  */
/* FILEDEFS FOR MESSAGE LIBRARIES                                   */
/*                                                                  */
'FILEDEF ISPMLIB DISK DUALMLIB MACLIB  * (PERM CONCAT'
'FILEDEF ISPMLIB DISK HRFMSG   MACLIB  * (PERM CONCAT'
'FILEDEF ISPMLIB DISK ISRNULL MESSAGE * (PERM CONCAT'
'FILEDEF ISPMLIB DISK ISRMLIB MACLIB * (PERM CONCAT'
'FILEDEF ISPMLIB DISK ISPMLIB MACLIB * (PERM CONCAT'
/*                                                                  */
/* FILEDEFS FOR SKELETON LIBRARIES                                  */
/*                                                                  */
'FILEDEF ISPSLIB DISK HRFSKEL  MACLIB  * (PERM CONCAT'
'FILEDEF ISPSLIB DISK ISRNULL SKELETON * (PERM CONCAT'
'FILEDEF ISPSLIB DISK ISRSLIB MACLIB * (PERM CONCAT'
/*                                                                  */
/* FILEDEFS FOR TABLE LIBRARIES                                     */
/*                                                                  */
'FILEDEF ISPTLIB DISK ISRNULL TABLE A (PERM CONCAT'
'FILEDEF ISPTLIB DISK TABLES MACLIB A (PERM CONCAT'
'FILEDEF ISPTLIB DISK ICHTLIB  MACLIB  * (PERM CONCAT'
'FILEDEF ISPTLIB DISK ISRTLIB MACLIB * (PERM CONCAT'
'FILEDEF ISPTLIB DISK ISPTLIB MACLIB * (PERM CONCAT'
/*                                                                  */
'FILEDEF ICHTABL DISK DUALTLIB MACLIB  * (PERM CONCAT'
/*                                                                  */
/* FILEDEF FOR LOAD LIBRARY                                         */
/*                                                                  */
'FILEDEF ISPLLIB DISK ICHSPF00 LOADLIB * (PERM CONCAT'
/*                                                                  */
/* FILEDEF FOR ISPF LOG/LIST FILE                                   */
/*                                                                  */
'FILEDEF ISPFILE DISK SPFCNTL1 EXEC    A (PERM LRECL 80 RECFM F'
```

Figure 10. Sample Filedefs for the ISPF EXEC for Systems with PDF

The concatenations required for RACF are:

- RACF ISPF library DUALPLIB MACLIB to the FILEDEF for ISPPLIB
- RACF ISPF library HRFPANL MACLIB to the FILEDEF for ISPPLIB
- RACF ISPF library DUALMLIB MACLIB to the FILEDEF for ISPMLIB
- RACF ISPF library HRFMSG MACLIB to the FILEDEF for ISPMLIB
- RACF ISPF library HRFSKEL MACLIB to the FILEDEF for ISPSLIB
- RACF ISPF library ICHTLIB MACLIB to the FILEDEF for ISPTLIB
- RACF ISPF library DUALTLIB MACLIB to the FILEDEF for ICHTABL

- The ICHSPF00 LOADLIB file to the FILEDEF for ISPLLIB
- The SPFCNTL1 EXEC file to the FILEDEF for ISPFILE

6.20.1.2 Step 2 - Modify the ISPF EXEC ISPDCS Line

If PDF is installed on your system, modify the following line of the ISPF EXEC:

```
'ISPDCS ISPDCSS ISPVM PANEL(ISR@PRIM) NEWAPPL(ISR) DMMMODE(T)' ISPFPARM
```

to look like this:

```
'ISPDCS ISPDCSS ISPVM PANEL(ISR@PRIM) NEWAPPL(ISR) DMMMODE(T) OPT('ISPFPARM')'
```

6.20.1.3 Step 3 - Modify RACF ISPF-Supplied Files

If your installation has PDF installed, and **you want to use the ISPF/PDF browse facility** (rather than XEDIT under CMS), you must modify panel ICHP00 in the RACF ISPF library, DUALPLIB.

In order to use PDF browse, specify &ICHXEDIT='NO' in the ICHP00 COPY file. (The default on the panel is &ICHXEDIT='YES', which provides XEDIT capability).

To update ICHP00 COPY, do a VMSES/E local modification to it.

Follow the steps documented in B.2, “Full Part Replacement (Not Assemble) - Example” on page 99 to perform the local modification to the ICHP00 COPY file. Use the following substitution values:

- For *fn* use **ICHP00**
- For *ft* use **COPY**
- For *ft-abbrv* use **CPY**
- For *nnnn* use **0001**
- For *blist* use **RPIBLDPL**
- For *memname* use **ICHP00**

At the end of the procedure your modified copy of ICHP00 COPY is in the DUALPLIB MACLIB on 6VMRAC10's 599 test build disk.

Where to next?

Continue with 6.20.3, “Modify the ISPF Primary Option Panel” on page 66.

6.20.2 Modify the ISPF Files for use with non-PDF

6.20.2.1 Step 1 - Modify the ISPSTART EXEC Filedefs

If PDF is not installed on your system, modify your ISPSTART EXEC as shown in Figure 11.

```
/*                                                                 */
/* FILEDEFS FOR PANEL LIBRARIES                                    */
/*                                                                 */
'filedef ispplib disk dualplib maclib * (perm concat'
'filedef ispplib disk hrfpanl maclib * (perm concat'
'filedef ispplib disk ispplib maclib * (perm concat'
/*                                                                 */
/* FILEDEFS FOR MESSAGE LIBRARIES                                  */
/*                                                                 */
'filedef ispmlib disk dualmlib maclib * (perm concat'
'filedef ispmlib disk hrfmsg maclib * (perm concat'
'filedef ispmlib disk ispmlib maclib * (perm concat'
/*                                                                 */
/* FILEDEFS FOR SKELETON LIBRARIES                                 */
/*                                                                 */
'filedef ispslib disk hrfskel maclib * (perm concat'
/*                                                                 */
/* FILEDEFS FOR TABLE LIBRARIES                                    */
/*                                                                 */
'filedef isptlib disk ispnull table a (perm concat'
'filedef isptlib disk ichtlib maclib * (perm concat'
'filedef isptlib disk isptlib maclib * (perm concat'
/*                                                                 */
'filedef ichtabl disk dualtlib maclib  * (perm concat'
/*                                                                 */
/* FILEDEF FOR LOAD LIBRARY                                        */
/*                                                                 */
'filedef ispllib disk ichspf00 loadlib * (perm concat'
/*                                                                 */
/* FILEDEF FOR ISPF LOG/LIST FILE                                  */
/*                                                                 */
'FILEDEF ISPFILE DISK SPFCNTL1 EXEC    A (PERM LRECL 80 RECFM F'
```

Figure 11. Sample Filedefs for the ISPSTART EXEC for Systems without PDF

The concatenations required for RACF are:

- RACF ISPF library DUALPLIB MACLIB to the FILEDEF for ISPPLIB
- RACF ISPF library HRFPANL MACLIB to the FILEDEF for ISPPLIB
- RACF ISPF library DUALMLIB MACLIB to the FILEDEF for ISPMLIB
- RACF ISPF library HRFMSG MACLIB to the FILEDEF for ISPMLIB
- RACF ISPF library HRFSKEL MACLIB to the FILEDEF for ISPSLIB
- RACF ISPF library ICHTLIB MACLIB to the FILEDEF for ISPTLIB
- RACF ISPF library DUALTLIB MACLIB to the FILEDEF for ICHTABL

- The ICHSPF00 LOADLIB file to the FILEDEF for ISPLLIB
- The SPFCNTL1 EXEC file to the FILEDEF for ISPFILE

6.20.2.2 Step 2 - Modify the ISPF EXEC ISPDCS Line

If PDF is not installed on your system, modify the following line of the ISPSTART EXEC:

```
'ISPDCS ISPDCSS ISPVM 'argstring
```

to look like this:

```
'ISPDCS ISPDCSS ISPVM PANEL(ISP@PRIM) OPT('argstring')'
```

Note: After you modify the ISPF EXEC, you might receive the following messages during execution of the RACF panels:

```
DMSOPN002E File PASRTLIB LOADLIB * not found
DMSOPN002E File VSPASCAL TXTLIB * not found
```

If this occurs, change the SCLM SWITCH=YES in the ISPF EXEC to SCLM SWITCH=NO. For more information, refer to ISPF information APAR II08650.

6.20.2.3 Step 3 - Modify RACF ISPF-Supplied Files

Procedural Note

If you do not have ISPF/PDF installed, follow the instructions in this section.

6.20.2.3.1 Update ICHSFSIN EXEC:

If PDF is not installed, remove the PDF dependency by ensuring that `ichpdf = "NO"` is in the ICHSFSIN EXEC.

To update ICHSFSIN EXEC, do a VMSES/E local modification to it.

Follow the steps documented in B.2, “Full Part Replacement (Not Assemble) - Example” on page 99 to perform the local modification to the ICHSFSIN EXEC file. Use the following substitution values:

- For *fn* use **ICHSFSIN**
- For *ft* use **EXEC**
- For *ft-abbrv* use **EXC**
- For *nnnn* use **0001**
- For *blist* use **RPIBL599**
- For *memname* use **ICHSFSIN**

At the end of the procedure your modified copy of ICHSFSIN EXEC is on 6VMRAC10's 599 test build disk.

6.20.2.3.2 Update RACF EXEC:

If you do not have PDF installed, modify the INIT routine in the RACF EXEC as shown in Figure 12 on page 65.

Follow the steps documented in B.2, “Full Part Replacement (Not Assemble) - Example” on page 99 to perform the local modification to the RACF EXEC file. Use the following substitution values:

- For *fn* use **RACF**
- For *ft* use **EXEC**.
- For *ft-abbrv* use **EXC**
- For *nnnn* use **0001**
- For *blist* use **RPIBL599**
- For *memname* use **RACF**

At the end of the procedure your modified copy of RACF EXEC is on 6VMRAC10's 599 test build disk.

The following example shows what needs to be changed. The changes are denoted by the highlighted, commented out, commands.

Note: This exec has been converted from EXEC2 to REXX™.

```
INIT:
Address 'COMMAND'                /* Point to cmd processor       */

/*   Note highlighted, commented out, commands                    */
/*                                                                */
/* first filedef the RACF and ISPF panel libraries                */

"filedef ispplib disk dualplib maclib * (perm concat"
"filedef ispplib disk hrfpanl maclib * (perm concat"
/*                                                                */
/* "filedef ispplib disk isrplib maclib * (perm concat"           */
/*                                                                */
"filedef ispplib disk ispplib maclib * (perm concat"

/* next, filedef the RACF and ISPF message libraries              */

"filedef ispmlib disk dualmlib maclib * (perm concat"
"filedef ispmlib disk hrfmsg  maclib * (perm concat"
"filedef ispmlib disk isrmlib maclib * (perm concat"
"filedef ispmlib disk ispmlib maclib * (perm concat"

/* now, filedef the RACF and ISPF skeleton libraries              */
"filedef ispslib disk hrfskel maclib * (perm concat"
"filedef ispslib disk ispslib maclib * (perm concat"
/*                                                                */
/* "filedef ispslib disk isrslib maclib * (perm concat"           */
/*                                                                */

/* now, filedef the RACF and ISPF table libraries                 */
"filedef isptlib disk isptlib maclib * (perm concat"
"filedef ichtabl disk dualtlib maclib * (perm concat"            */

/* now, filedef the ISPF userprof maclib                          */
"filedef ispprof disk userprof maclib a (perm lrecl 80 recfm f"

/* now, filedef the RACF EXEC file                                */
"filedef ispfile disk spfcntl1 exec a (perm lrecl 80 recfm f"

/* now, filedef the the RACF panel driver load library            */
"filedef ispllib disk ichspf00 loadlib * (perm lrecl 13000 recfm u"

Address                          /* Reset envir to default       */
/* now, go to the ISPF PRIMARY OPTION panel with option(R) for RACF */

/******  Replace the following line                               */
/* "ISPDCS ISPDCSS ISPVM PANEL(ISR@PRIM) OPT(R)" */
/***** with                                                       */
"ISPDCS ISPDCSS ISPVM PANEL(ISP@PRIM) OPT(R)"

 Address 'COMMAND' msgvals       /* Restore system settings     */
Exit rc
```

Figure 12. Changes for RACF EXEC INIT Routine for Systems without PDF

6.20.3 Modify the ISPF Primary Option Panel

A sample ISPF Primary Option Panel (ISRPRIM SAMPLE) is supplied on the 6VMRAC10 599 test build disk. It includes entries for modifying your panel.

Under `%OPTION  ===>_ZCMD` there is an entry:

```
%   R +RACF        - RACF security panels
```

and under

```
)PROC
  &ZSEL = TRANS( TRUNC (&ZCMD,'.')
```

an entry:

```
R,'CMD(EXEC RACF ISPF) NEWAPPL(ICH)'
```

These statements put an option for RACF on the ISPF Primary Option Panel.

6.20.4 Dual Registration Users Only

Procedural Note

If you are not using dual registration or you are doing dual registration using DirMaint, skip to 6.20.5, “Invoke the RACF ISPF Panels” on page 67.

6.20.4.1 Set Defaults in PROFILE

The installation of the RACF ISPF panels loads the DUALREG PROFILE file. This file contains default settings for certain fields on the dual registration panels.

To update DUALREG PROFILE you need to do a VMSES/E local modification to it.

Follow the steps documented in B.2, “Full Part Replacement (Not Assemble) - Example” on page 99 to perform the local modification to the DUALREG PROFILE file. Use the following substitution values:

- For *fn* use **DUALREG**
- For *ft* use **PROFILE**
- For *ft-abbrv* use **PRF**
- For *nnnn* use **0001**
- For *blist* use **RPIBL599**
- For *memname* use **DUALREG**

At the end of the procedure your modified copy of DUALREG PROFILE will be on 6VMRAC10's 599 test build disk.

6.20.4.2 Verify directory entries

The file DUALREG SKELETON is used by dual registration to create user directory entries. The directory statements in this file are included in each directory entry created by dual registration. You need to make sure its contents are suitable to your installation.

To modify the DUALREG SKELETON file, do a VMSES/E local modification to it.

Follow the steps documented in B.2, "Full Part Replacement (Not Assemble) - Example" on page 99 to perform the local modification to the DUALREG SKELETON file. Use the following substitution values:

- For *fn* use **DUALREG**.
- For *ft* use **SKELETON**
- For *ft-abbrv* use **SKL**.
- For *nnnn* use **0001**
- For *blist* use **RPIBL599**
- For *memname* use **DUALREG**

At the end of the procedure your modified copy of DUALREG SKELETON will be on 6VMRAC10's 599 test build disk.

6.20.5 Invoke the RACF ISPF Panels

In a CMS environment, invoke the RACF ISPF panels by entering either:

```
RACF (PANEL
```

or

```
ISPF R
```

Either command initializes ISPF and then invokes ISPF with option(R).

In ISPF, selection of option 6 allows you to enter EXECs and CMS and CP commands. From option 6, you can enter `RACF ISPF` to invoke ISPF option(R).

Note: Because the RACF EXEC initializes ISPF, the FILEDEFs in the RACF EXEC must be identical to the FILEDEFs in the installation's ISPF EXEC.

6.21 Task 19. Place RACF Into Production

Procedural Note

All customers should perform this step.

6.21.1 Copy RACF Files Into Production

Once you are satisfied with your testing of the RACF code using the RACMAINT user ID, you must copy the production files to the RACFVM user ID.

1 Log on to MAINT to put RACF code on to the production build disks.

2 If you have RACF installed into shared file (SFS) then you need to start the shared filepool server machines.

xautolog autolog1

3 This step will:

- Copy the RACF system code from the test build disk to RACFVM 305 production build disk.
- Copy the RACF CMS/CST files from the test build disk (6VMRAC10's 590) to the production build disk (RACFVM 490 disk) using the DDR process.
- Copy the RACF GCS files to your GCS production system disk.
- Puts RACF general use code on the 'Y' disk (MAINT's 19E disk).

put2prod

4 (Optional) If you did the optional install steps to set up the RACF ISPF Panels then copy the RACF ISPF panels from the test build disk to the ISPF system disk.

link 6VMRAC10 599 599 rr
access 599 e
access *ispf-fm* **f**

Where *ispf-fm* is the ISPF product system disk. The default is ISPVM 192.

vmfcopy * * e = = f (prodid 6VMRAC10%RACF olddate replace

The VMFCOPY command updates the VMSES PARTCAT file on the ISPF code disk.

5 (Optional) If you want to use the RACF ISPF code, copy the ISPF general use code on to the 'Y' disk (MAINT's 19E disk).

a Log on to MAINT.

b Copy the ISPF general user code.

link 6VMRAC10 599 599 rr
access 599 e
access 19e f

The VMFCOPY command updates the VMSES PARTCAT file on the 19E disk.

```
vmfcopy RACF EXEC e = = f2 (prodid 6VMRAC10%RACF olddate replace
vmfcopy ICHSPF00 LOADLIB e = = f2 (prodid 6VMRAC10%RACF olddate replace
vmfcopy DUALREG PROFILE  e = = f2 (prodid 6VMRAC10%RACF olddate replace
vmfcopy DUALREG SKELETON e = = f2 (prodid 6VMRAC10%RACF olddate replace
```

6 Set up the AUTOLOG1 and AUTOLOG2 user IDs.

Procedural Note

Customers doing new installs should perform this step. (Note, it is possible that these user IDs are already set up if you migrated these user IDs during any system migration tasks.)

Note: If you have changed AUTOLOG1 to another user ID, substitute the new user ID for all references to AUTOLOG1 in this program directory.

AUTOLOG1 normally logs on all service machines automatically. To get maximum security protection from RACF, AUTOLOG1 should allow **only** the RACF service machine (RACFVM) to be logged on. This prevents other products from being logged on before RACF is initialized.

If your installation has functions that are automatically logged on by AUTOLOG1, you should move those functions to AUTOLOG2.

Include the following in the PROFILE EXEC of AUTOLOG1:

```
XAUTOLOG RACFVM
```

During CP initialization, AUTOLOG1 logs on RACFVM, which then logs on AUTOLOG2. AUTOLOG2 then logs on its contents.

7 Initialize RACF from the system operator's console.

```
force 6VMRAC10
force MAINT
force RACMAINT
xautolog RACFVM
```

8 At this time your system is still IPL'ed off of the secondary parm disk (CF2). The next time you IPL, you will IPL from the primary parm (CF1) disk; which is the default for IPL. If you want to, you can shutdown and IPL your VM system at this time.

RACF is now installed and built on your system.

7.0 Service Instructions

Note - z/VM Automated Service Procedure

The **preferred** method for installing service to RACF is to use the z/VM automated service procedure (use of the **SERVICE** and **PUT2PROD** commands).

If you have chosen to use the automated procedure to apply preventive (RSU) and CORrective service to your z/VM system, you need to follow the service instructions documented in the *z/VM: Guide for Automated Installation and Service* manual, instead of those presented here.

Attention - RSU Note

If you are applying a RACF RSU, follow the instructions in Appendix A, "Applying an RSU for RACF" on page 89. You will return to a step in this chapter as specified in that appendix.

This section of the program directory contains the procedure to install CORrective service to RACF. VMSES/E is used to install service for RACF.

To become more familiar with service using VMSES/E, you should read the introductory chapters in *VMSES/E Introduction and Reference*. This manual also contains the command syntax for the VMSES/E commands listed in the procedure.

Note: Each task in the service instructions must be performed. Each step of each task must be followed. Do not skip any step unless directed to do so. All instructions showing accessing of disks assume the use of default minidisk addresses. If you are using different minidisk addresses, or if you are using a shared file system, change the instructions appropriately.

7.1 VMSES/E Service Process Overview

The following is a brief description of the main steps in servicing RACF using VMSES/E.

- Receive Service

  The VMFREC command receives service from the delivery media and places it on the Delta disk.

- Merge Service

Use the VMFMRDSK command to clear the alternate apply disk before receiving new service. This allows you to easily remove the new service if a serious problem is found.

- Apply Service

  The VMFAPPLY command updates the version vector table (VVT), which identifies the service level of all the serviced parts. In addition, AUX files are generated from the VVT for parts that require them.

- Reapply Local Service (if applicable)

  All local service (mods) must be entered into the software inventory to allow VMSES/E to track the changes and build them into the system. Refer to Chapter 7 in the *z/VM Service Guide* for this procedure.

- Build New Levels

  The build task generates the serviced level of an object and places the new object on a test BUILD disk.

- Place the New Service into Production

  Once the service is satisfactorily tested it should be put into production by copying the new service to the production disk.

7.2 Servicing RACF

7.2.1 Task 1. Prepare to Receive Service

Electronic Service (envelope file)

If you have received the service electronically or on CD-ROM, follow the appropriate instructions to retrieve and decompress the envelope file to your A-disk. The decompression is currently done by using the DETERSE MODULE (shipped with VMSES/E).

The documentation envelope and the service (PTF) envelope files must have a file type of SERVLINK. Make note of the file names that you are using as you will need to enter them in place of the variable *envfilename* in the VMFREC commands that follow.

The *ppfname* used throughout these servicing instructions is **6VMRAC10**, which assumes you are using the PPF supplied by IBM for RACF. If you have your own PPF override file for RACF, you should use your file's *ppfname* instead of **6VMRAC10**. The *ppfname* you use should be used **throughout** the rest of this procedure, unless otherwise stated differently.

The *compname* used throughout these servicing instructions is **RACF**or **RACFSFS**, which assumes you are using the component name within the 6VMRAC10 PPF file. If you specify your own *ppfname*, you should use the *compname* from that file instead of **RACF** or **RACFSFS**. The *compname* you use should be used **throughout** the rest of this procedure.

1 Log on to RACF service user ID **6VMRAC10**.

2 Establish access to the software inventory disk.

Note: If the MAINT 51D minidisk was accessed R/O, you will need to have the user that has it accessed R/W link it R/O. You then can issue the following commands to obtain R/W access to it.

link MAINT 51d 51d mr
access 51d d

The 51D minidisk is where the VMSES/E Software Inventory files and other product-dependent files reside.

3 Have the RACF CORrective service tape mounted and attached to **6VMRAC10** at virtual address 181. If you have the CORrective service envelope (SERVLINK) file, make sure that it is available on the A-disk or any minidisk or SFS directory accessed as file mode C.

4 Establish the correct minidisk access order.

vmfsetup 6VMRAC10 {RACF | RACFSFS}

6VMRAC10 is the PPF that was shipped with the product. If you have your own PPF override you should substitute your PPF name for 6VMRAC10.

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

5 Receive the documentation. VMFREC, with the INFO option, loads the documentation and displays a list of all the products on the tape.

a If receiving the service from tape

vmfrec info

This command loads the service memo to the 191 disk.

b If receiving the service from an envelope file

vmfrec info (env *envfilename*

envfilename is the file name of the documentation envelope (SERVLINK) file.

This command loads the service memo to the 191 disk.

6 Check the receive message log ($VMFREC $MSGLOG) for warning and error messages.

vmfview receive

Also make note of which products and components have service on the tape. To do this, use the PF5 key to show all status messages which identify the products on the tape.

7 Clear the alternate APPLY disk to ensure that you have a clean disk for new service.

vmfmrdsk 6VMRAC10 {RACF | RACFSFS} apply

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

This command clears the alternate APPLY disk.

8 Review the merge message log ($VMFMRD $MSGLOG). If necessary, correct any problems before going on. For information about handling specific error messages, see *z/VM: System Messages and Codes*, or use on-line HELP.

vmfview mrd

7.2.2 Task 2. Receive the Service

1 Receive the service.

Note: If you are installing multiple service tapes, you can receive all of the service for this prodid before applying and building it.

For **each** service tape or electronic envelope you want to receive repeat the respective vmfrec command.

a If receiving the service from tape

vmfrec ppf 6VMRAC10 {RACF | RACFSFS}

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

This command receives service from your service tape. All new service is loaded to the DELTA disk.

b If receiving the service from the PTF envelope file

vmfrec ppf 6VMRAC10 {RACF | RACFSFS} (env *envfilename*

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

envfilename is the file name of the service (PTF) envelope (SERVLINK) file.

This command receives service from your service envelope. All new service is loaded to the DELTA disk.

2 Review the receive message log ($VMFREC $MSGLOG). If necessary, correct any problems before going on. For information about handling specific error messages, see *z/VM: System Messages and Codes*, or use on-line HELP.

vmfview receive

7.2.3 Task 3. Apply the Service

1 Apply the new service.

vmfapply ppf 6VMRAC10 {RACF | RACFSFS}

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

This command applies the service that you just received. The version vector table (VVT) is updated with all serviced parts and all necessary AUX files are generated on the alternate apply disk.

You must review the VMFAPPLY message log if you receive a return code (RC) of a 4, as this may indicate that you have local modifications that need to be reworked.

2 Review the apply message log ($VMFAPP $MSGLOG). If necessary, correct any problems before going on. For information about handling specific error messages, see *z/VM: System Messages and Codes*, or use on-line HELP.

vmfview apply

Attention

If you get the message VMFAPP2120W, rework any local modifications before building the new RACF. Refer to chapter 7 in *z/VM Service Guide*. Follow the steps that are applicable to your local modification. For local modifications applied during initial installation also refer to Appendix B, “RACF Local Modifications - Examples” on page 97, to see how the local modification was put on.

Use the following substitution values:

- **zvm** should be **6VMRAC10**.
- *compname* should be **RACF** (for installing on minidisks), or **RACFSFS** (for installing in SFS directories),
- *fm-local* should be the file mode of the 2C2 disk.
- *localmod* should be **localsam**

If you have changed any of the installation parameters through a PPF override, you need to substitute your changed values where applicable.

Keep in mind that when you get to the "Rebuild Remaining Objects" step in *z/VM Service Guide*, you should return back to this program directory at 7.2.4, “Task 4. Update the Build Status Table” on page 77.

7.2.4 Task 4. Update the Build Status Table

1 Update the build status table with serviced parts.

vmfbld ppf 6VMRAC10 {RACF | RACFSFS} (status

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

This command updates the build status table.

Attention

If the $PPF files have been serviced you get the following prompt:

```
VMFBLD2185R The following source product parameter files have been
            serviced:
VMFBLD2185R 6VMRAC10 $PPF
VMFBLD2185R When source product parameter files are serviced, all
            product parameter files built from them must be recompiled
            using VMFPPF before VMFBLD can be run.
VMFBLD2185R Enter zero (0) to have the serviced source product
            parameter files built to your A-disk and exit VMFBLD so
            you can recompile your product parameter files with VMFPPF.
VMFBLD2185R Enter one (1) to continue only if you have already
            recompiled your product parameter files with VMFPPF.
```

0

Enter a 0 and complete the following steps before you continue.

```
VMFBLD2188I Building 6VMRAC10 $PPF
            on 191 (A) from level $PFnnnnn
```

vmfppf 6VMRAC10 *

Note: If you have created your own PPF override, use your PPF name instead of 6VMRAC10.

copy 6VMRAC10 $PPF a = = d (olddate replace
erase 6VMRAC10 $PPF a

Note: Do not use your own PPF name in place of 6VMRAC10 for the COPY and ERASE commands.

vmfbld ppf 6VMRAC10 {RACF | RACFSFS} (status

1

Reissue VMFBLD to complete updating the build status table. If you have your own PPF name then use it on the VMFBLD command.

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

When you receive the prompt that was previously displayed, enter a 1 to continue.

2 Use VMFVIEW to review the build status messages, and see what objects need to be built.

vmfview build

7.2.5 Task 5. Build Serviced Objects

1 Rebuild RACF serviced parts.

vmfbld ppf 6VMRAC10 {RACF | RACFSFS} (serviced

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

2 Review the build message log ($VMFBLD $MSGLOG). If necessary, correct any problems before going on. For information about handling specific error messages, see *z/VM: System Messages and Codes*, or use on-line HELP.

vmfview build

3 If you received message VMFBDU2180I that stated a status of 'REBUILD CP NUCLEUS', you need to rebuild the CP Nucleus. This is because HCPRPI, HCPRPD, HCPRPF, HCPRPW or HCPRWA was changed by RACF service.

The following steps should be followed to get the new RACF serviced HCP*xxx* files into the CP nucleus.

a Log on to the CP maintenance ID (the default is the MAINT user ID).

b Set up the CP disk access order.

vmfsetup zvm cp

zvm is the default PPF for z/VM version 6. If you have a PPF override, substitute your override name.

c Copy or replace the HCP*xxx* RPIBASE0 files from 6VMRAC10's 505 test build disk to the CP local modification disk (the default is MAINT's 2C4 disk).

link 6VMRAC10 505 505 rr
acc 505 z
listfile hcp* rpibase0 z (exec args
exec cms copyfile % = = *fm-2c4* **(oldd replace**

d If you are using Common Criteria LSPP-conformant version of HCPRWA (which is HCPRWAC), as documented in the *z/VM: Secure Configuration Guide*, then issue the following commands. If not, then skip this step.

erase hcprwa rpibase0 *fm-2c4*
rename hcprwac rpibase0 *fm-2c4* **hcprwa = =**

e Copy the RACF MACLIB from the 6VMRAC10 505 test build disk to your normal CP maintenance 19E disk (in case the RACF MACLIB was also serviced).

Note: Make sure you use a file mode of 2 on the vmfcopy command.

vmfcopy racf maclib z = = *fm-19E***2 (prodid 6VMRAC10%RACF olddate replace**

f Assemble the HCPRPD, HCPRPF, HCPRPG, HCPRPI, HCPRPW, and HCPRWA modules. Issue the VMFHLASM for each HCP*xxx* file.

vmfhlasm hcprpf zvm cp ($select outmode localmod
vmfhlasm hcprpg zvm cp ($select outmode localmod
vmfhlasm hcprpi zvm cp ($select outmode localmod
vmfhlasm hcprwa zvm cp ($select outmode localmod
vmfhlasm hcprpw zvm cp ($select outmode localmod
vmfhlasm hcprpd zvm cp ($select outmode localmod

Where *zvm* is the default PPF for z/VM version 6. If you have a PPF override, substitute your override name.

g Generate or build the CP Nucleus.

vmfbld ppf zvm cp (serviced

zvm is the default PPF for z/VM version 6. If you have a PPF override, substitute your override name.

h Verify the CP load map by XEDITing CPLOAD MAP to check for any unresolved or undefined references.

i Copy the new CP nucleus to the primary parm disk and save a copy of your current CPLOAD MODULE. See *z/VM Service Guide* for information on copying to the parm disk.

4 If part RACFVM NUCLEUS was serviced, perform these additional steps:

a Log on to the 6VMRAC10 user ID.

b Generate a new RACF CMS nucleus

```
def 590 490
def 505 305
acc 305 e
gennuc
```

c The following screens appear:

```
A modified version of CMS is about to be generated.
```

```
The modified CMS nucleus must be generated with a virtual machine
size of 21M.

The GENNUC EXEC will automatically set the virtual machine size to
21M and IPL the modified nucleus.

Note:  Please reply to the DMSINQ609R Message by Entering:   32
```

Note: The number displayed is dependent on the type of DASD your installation has (it might not be 32).

Type in the number that appears and press Enter to continue the IPL.

The IPL might take a few minutes, depending on your system setup. RACF's modified CMS is IPLed as it is being written to DASD.

A copy of the CMS nucleus map will be placed in your reader. Receive the file and keep it for use in future problem determination.

d Reset the environment

```
def 490 590
def 305 505
acc 590 t
vmfsetup 6VMRAC10 {RACF | RACFSFS}
```

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

5 If part IRRTEMP1 COPY was serviced, update the RACF database templates by following these additional steps.

Note: If you are sharing a RACF database, understand the considerations in 5.2.5, “Sharing a RACF Database” on page 12.

Be sure to run RACFCONV against each primary and backup database on your system.

To convert the database templates from a VM system:

a Make sure that RACF is not running.

b Run RACFCONV EXEC to convert the templates.

link RACFVM 200 200 wr
racfconv

```
This exec is used to run the Racf utility IRRMIN00 to
convert existing Racf datasets for a new release of Racf.

Press ENTER to continue....
```

ENTER

```
Enter the device address to be converted
```

200

```
About to update templates in 'RACF.DATASET' at virtual address '200'
Do you wish to continue?

Enter YES or NO
```

yes

```
Processing begins
All output will be placed in the MIN00U OUTPUT file on the 'A' disk.
Program 'IRRMIN00' is being executed - Please wait -


Processing complete
Return code from 'IRRMIN00' = 0
Ready; T=0.07/0.10 11:41:46
```

link RACFVM 300 300 wr
racfconv

```
This exec is used to run the Racf utility IRRMIN00 to
convert existing Racf datasets for a new release of Racf.

Press ENTER to continue....
```

ENTER

```
Enter the device address to be converted
```

300

```
About to update templates in 'RACF.BACKUP' at virtual address '300'
Do you wish to continue?

Enter YES or NO
```

yes

```
Processing begins
All output will be placed in the MIN00U OUTPUT file on the 'A' disk.
Program 'IRRMIN00' is being executed - Please wait -


Processing complete
Return code from 'IRRMIN00' = 0
Ready; T=0.07/0.10 11:44:44
```

det 200
det 300

To convert the database templates from a z/OS system, see *z/VM: RACF Security Server System Programmer's Guide*.

6 If parts ICHPERM TEXT or ICHPERMT TEMPLATE have been serviced and you have enabled RACF OpenExtensions support, copy part ESMLIB CSLLIB from the 505 disk to the SFS file pool server's 'A' disk.

7 If part PROFILE SAMPLE has been serviced, copy the PROFILE SAMPLE file to RACFVM's A-disk and RACMAINT's A-disk.

link RACFVM 191 199 MR
acc 199 Z
copyfile profile sample *fm-505* **profile exec z**
det 199
link RACMAINT 191 199 MR
acc 199 Z
copyfile profile sample *fm-505* **profile exec z**
det 199

Where *fm-505* is the current file mode of 6VMRAC10's 505 test build disk.

8 If part SMF CONTROL has been serviced, copy the SMF CONTROL file to RACFVM's A-disk and RACMAINT's A-disk.

link RACFVM 191 199 MR
acc 199 Z
copyfile smf control *fm-505* **smf control z**
det 199
link RACMAINT 191 199 MR
acc 199 Z
copyfile smf control *fm-505* **smf control z**
det 199

Where *fm-505* is the current file mode of 6VMRAC10's 505 test build disk.

7.2.6 Task 6. IPL the CP System and Test RACF Service

Before you place the new service into production you should test it out to make sure it works. You can use the test or backup server user ID RACMAINT.

IPL your system with the NOAUTOLOG option. After the system IPL, XAUTOLOG the RACMAINT user ID, which initializes RACF.

If ICHRDSNT was serviced and RACF cannot find the database name in the database name table (ICHRDSNT) during initialization, it might be for one of the following reasons:

- The database name specified in ICHRDSNT does not match the data set name on the database DASD volumes.
- The database name contains an asterisk (*).
- No FILEDEF exists for the RACF database.

In each instance, the system prompts the system operator for a RACF database name.

From the system operator's console, do **one** of the following:

Enter: `SEND RACFVM 1racf.dataset`

where *racf.dataset* is your installation's RACF database name

or

Enter: `SEND RACFVM 1NONE`

Note: If you specify `SEND RACFVM 1NONE`, RACF is not active for this IPL. This is not recommended, because no one will be able to log on to the system.

7.2.7 Task 7. Copy the New RACF Serviced Files Into Production

Once you are satisfied with your testing of the RACF code using the RACMAINT user ID, you must copy the production files to the RACFVM user ID.

1 Log on to 6VMRAC10 to put RACF code on to the production build disks.

2 Copy the RACF system code from the test build disk to the RACFVM 305 production build disk.

access 505 e
link RACFVM 305 305 mr
access 305 f
vmfcopy * * e = = f (prodid 6VMRAC10%RACF olddate replace

The VMFCOPY command updates the VMSES PARTCAT file on the 305 disk.

3 Copy the RACF CMS/CST files from the test build disk (6VMRAC10's 590) to the production build disk RACFVM 490 disk using DDR process.

a Link and access RACF's test and production minidisks.

access 590 t
link RACFVM 490 490 mr
access 490 v

b Do the DDR copy.

ddr

```
z/VM DASD DUMP/RESTORE PROGRAM
ENTER:
```

	The system prompts you to enter a DDR control statement.
sysprint cons	Route messages to the console (rather than a printer).
`ENTER:`	Enter 590 as the source minidisk for the DDR.
input 590 dasd *590-label*	Enter the label of 6VMRAC10's 590 minidisk for *590-label* (for example, RAC590). 590 is the virtual device number of the test RACF system disk. **dasd** causes DDR to determine the device type of the real DASD volume on which the 590 minidisk resides (for example, 3380).
`ENTER:`	Enter 490 as the target minidisk for the DDR.
output 490 dasd *490-label*	Enter the label of RACFVM's 490 minidisk for *490-label* (for example, RVM490). 490 is the virtual device number of the production RACF system disk you are creating. **dasd** causes DDR to determine the device type of the real DASD volume on which the 490 minidisk resides. The 490 disk must be the same DASD type as the 590 disk.
`ENTER:`	Enter the COPY control statement to copy the entire 590 minidisk.
copy all	

`COPYING` *590-label*
⋮
`END OF COPY`
`ENTER:`
	DDR copies and displays messages about the operation. When the processing is complete, DDR prompts you to enter another control statement.

ENTER	At the prompt, press ENTER to enter a null line.
`END OF JOB` `Ready; T=`*n.nn/n.nn hh:mm:ss*	The system reports end-of-job status.

C Relabel the 490 minidisk as *490-label*. When you copied the 590 minidisk to the 490 minidisk, the DDR program copied the 590 minidisk label also.

access 490 r
format 490 r (label

```
DMSFOR605R Enter disk label:
```

490-label

Enter the original label of RACFVM's 490 minidisk for *490-label* (for example, RVM490) to change the label of the 490 disk.

Access 490 read/write. You **must** use the LABEL option. If you do not, you will erase all of the files on the 490 minidisk.

4 (Optional) If you use GCS, copy the RACF GCS files to your GCS disk.

access 29e e
access *gcs-fm* **f**
vmfcopy rpigcs loadlib e = = f (prodid 6VMRAC10%RACF olddate replace
vmfcopy rpicdx loadlib e = = f (prodid 6VMRAC10%RACF olddate replace

gcs-fm is the GCS production system disk. The default is MAINT 193. If you copy to MAINT 193 you also need to copy these files to MAINT 493, which is the GCS test build disk.

The VMFCOPY command updates the VMSES PARTCAT file on the ISPF code disk.

5 (Optional) If you are using the RACF ISPF code copy the RACF ISPF code from the test build disk to the ISPF system disk.

access 599 e
access *ispf-fm* **f**
vmfcopy * * e = = f (prodid 6VMRAC10%RACF olddate replace

ispf-fm is the ISPF product system disk. The default is ISPVM 192.

The VMFCOPY command will update the VMSES PARTCAT file on the ISPF code disk.

6 (Optional) If you installed the RACF ISPF code, copy the ISPF general use code to the 'Y' disk (MAINT's 19E disk).

a Log on to MAINT.

b If the English ISPF code is installed, copy the ISPF general user code.

```
link 6VMRAC10 599 599 rr
access 599 e
access 19e f
vmfcopy RACF EXEC e = = f2 (prodid 6VMRAC10%RACF olddate replace
vmfcopy ICHSPF00 LOADLIB e = = f2 (prodid 6VMRAC10%RACF olddate replace
vmfcopy DUALREG PROFILE  e = = f2 (prodid 6VMRAC10%RACF olddate replace
vmfcopy DUALREG SKELETON e = = f2 (prodid 6VMRAC10%RACF olddate replace
```

The VMFCOPY command updates the VMSES PARTCAT file on the 19E disk.

7 Log on to MAINT if you plan to put RACF general use code on the 'Y' disk (MAINT's 19E disk). Or log on to the owner of the disk that will contain the 'production' level of the RACF code.

```
link 6VMRAC10 29e 29e rr
access 29e e
access 19e f
vmfcopy * * e = = f2 (prodid 6VMRAC10%RACF olddate replace
```

The VMFCOPY command updates the VMSES PARTCAT file on the 19E disk.

8 Re-save the CMS saved system, to return the 19E minidisk (Y-disk) to 'shared' status. See the section 'Placing (Serviced) Components into Production' in *z/VM Service Guide* for detailed information about how to save the CMS saved system.

9 Initialize RACF from the system operator's console.

```
force 6VMRAC10
force MAINT
force RACMAINT
xautolog RACFVM
```

You have finished servicing RACF.

Appendix A. Applying an RSU for RACF

Note - z/VM Automated Service Procedure

The **preferred** method for installing service to RACF is to use the z/VM automated service procedure (use of the **SERVICE** and **PUT2PROD** commands).

If you have chosen to use the automated procedure to apply preventive (RSU) and CORrective service to your z/VM system, you need to follow the service instructions documented in the *z/VM: Guide for Automated Installation and Service* manual, instead of those presented here.

The recommended service upgrade (RSU) is structured to install all PTFs included on the RSU plus the files containing the preapplied service and prebuilt objects. All PTF-related files are loaded to the delta disk. The file containing the preapplied service, that is, containing the results of VMFAPPLY, is loaded to the alternate apply disk and the contents of the tape files containing prebuilt objects are loaded to the appropriate build disks.

Points to consider about using the Product Service Upgrade procedure are:

- This process does not alter any of your tailored flat files (files serviced full part replacement only) in any way. Local modifiable assemble files you might have updated will have to be re-worked to include any new service to these files.
- Planning must be done (such as determining disk sizes, and determining what service, if any, on your existing system is not contained on the RSU) prior to actually loading the service from the RSU. These tasks will be discussed.

The following outline is an overview of what tasks need to be performed during the Product Service Update (PSU) procedure using the RSU:

- Prepare System

  In this task, you receive the documentation contained on the RSU and determine the DASD required to install the RSU.

- Merge Service

  Use the VMFMRDSK command to clear the alternate apply disk before receiving the RSU. This allows you to easily remove the new service if a serious problem is found.

- Receive Service

  The VMFINS command receives service from the RSU and places it on the Delta disk.

- Apply Additional Service

The VMFAPPLY command updates the version vector table (VVT), which identifies the service level of all the serviced parts. In addition, AUX files are generated from the VVT for parts that require them. These steps are used to reapply service that was not contained on the RSU that was already installed for RACF.

- Reapply Local Modifications (if applicable)

  All local modifications must be entered into the software inventory to allow VMSES/E to track the changes and build them into the system.

- Build New Levels

  The build task generates the serviced level of an object and places the new object on a BUILD disk.

- Place the New Service into Production

  Once the service is satisfactorily tested it should be put into production by copying the new service to the production disk.

A.1.1 Prepare Your System for Service Refresh

Electronic Service (envelope file)

If you have received the RSU electronically or on CD-ROM, follow the appropriate instructions to retrieve and decompress the envelope file to your A-disk. The decompression is currently done by using the DETERSE MODULE (shipped with VMSES/E).

The service (RSU PTF) envelope files must have a file type of SERVLINK. Make note of the file names that you are using as you will need to enter them in place of the variable *envfilename* in the VMFINS commands that follow.

The RSU documentation envelope file will be a readable flat file after DERTERSE is run against it. It will not get used in the following RSU application instructions.

The *ppfname* used throughout these instructions is **6VMRAC10**, which assumes you are using the PPF supplied by IBM for RACF. If you have your own PPF override file for RACF you should use your file's *ppfname* instead of **6VMRAC10**. The *ppfname* you use should be used **throughout** the rest of this procedure.

The *compname* used throughout these servicing instructions is **RACF** or **RACFSFS**. If you specify your own *ppfname*, you should use the *compname* from that file instead of **RACF** or, **RACFSFS**. The *compname* you use should be used **throughout** the rest of this procedure.

1 Read through the latest RSU information hard copy memo.

2. Log on to the RACF service user ID 6VMRAC10.

3. Establish write access to the Software Inventory disk if it is not already linked in write mode.

   Note: If the MAINT 51D minidisk was accessed R/O, you need to have the user who has it linked R/W link it as R/O. You then can issue the following commands to obtain write access to it. Do not use *mw* mode.

link MAINT 51d 51d mr **access 51d d**	The MAINT 51D disk is where the VMSES/E system level software inventory files reside.

4. Mount the RSU tape on the tape drive as virtual device 181. You must use 181. If you have the RSU in a service envelope (SERVLINK) file make sure that it is available on the A-disk or any minidisk or SFS directory accessed as file mode C.

5. Receive the documentation for the RSU.

   This step loads the cumulative apply status table (SRVAPPS) which identifies all preapplied service contained on the RSU. These files are loaded to the 51D disk.

   a. If receiving the RSU from tape

vmfins install info (nomemo

   b. If receiving the RSU from an envelope file

vmfins install info (nomemo env *envfilename*	*envfilename* is the file name of the service (RSU PTF) envelope file (SERVLINK) that represents volume 1 of the RSU.

6. Determine DASD sizes for the disks to receive service.

   In order to receive the service from the RSU, you need to have adequate space available on the alternate APPLY and DELTA disks. The required sizes are identified in the RACF documentation (6VMRAC10 MEMO D) received in the previous step.

7. Setup the correct minidisk access order.

vmfsetup 6VMRAC10 {RACF | RACFSFS}

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

8 Merge the APPLY disks for RACF.

Next, you must prepare your system to receive the service from the RSU. To do this, you must first clear the alternate apply disk for receipt of the service from the RSU.

Enter the VMFMRDSK command to merge the alternate apply disk to the apply disk. This will clear the alternate apply disk.

vmfmrdsk 6VMRAC10 {RACF | RACFSFS} apply

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

9 Obtain additional information about the service on the RSU and how it will affect your local modifications by invoking the VMFPSU command. This command creates an output file, ***appid* PSUPLAN**, which you can review. See *z/VM Service Guide* for an explanation of this file.

vmfpsu 6VMRAC10 {RACF | RACFSFS}

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

This command produces an output file that contains information about the service on the RSU compared against the service and local modifications on your system. The file name is ***appid* PSUPLAN**, where ***appid*** is specified in the PPF file.

Note: In the ***appid* PSUPLAN** file, the local modifications shown are only the ones that need to be reworked. All other local modifications to be rebuilt will be reflected in the created **PSU $SELECT** file. See step 3 on page 95 for more information on the **PSU $SELECT** file.

A.1.2 Receive the Preapplied, Prebuilt Service

1 Refresh the RACF service disks by loading new service from the RSU.

a If receiving the RSU from tape

vmfins install ppf 6VMRAC10 {RACF | RACFSFS} (nomemo nolink

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

b If receiving the RSU from an envelope file

vmfins install ppf 6VMRAC10 {RACF | RACFSFS} (nomemo nolink env *envfilename*

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

envfilename is the file name of the service (RSU PTF) envelope file (SERVLINK) that represents volume 1 of the RSU. If you have more than one envelope file for the RSU you will be prompted for them when needed.

```
VMFINS2601R Do you want to create an override for :PPF 6VMRAC10 RACF :PRODID
            6VMRAC10%RACF?
            Enter 0 (No), 1 (Yes) or 2 (Exit)
0
VMFINS2603I Processing product :PPF 6VMRAC10 RACF :PRODID 6VMRAC10%RACF
VMFREQ2805I Product :PPF 6VMRAC10 RACF :PRODID 6VMRAC10%RACF has passed
            requisite checking
VMFINT2603I Installing product :PPF 6VMRAC10 RACF :PRODID 6VMRAC10%RACF
VMFSET2760I VMFSETUP processing started for 6VMRAC10 RACF
VMFUTL2205I Minidisk|Directory Assignments:
            String    Mode  Stat  Vdev  Label/Directory
VMFUTL2205I LOCALSAM  E      R/W  2C2   2C2INS
VMFUTL2205I APPLY     F      R/W  2A6   2A6INS
VMFUTL2205I           G      R/W  2A2   2A2INS
VMFUTL2205I DELTA     H      R/W  2D2   2D2INS
VMFUTL2205I BUILD0    I      R/W  29E   29EINS
VMFUTL2205I BUILD6    J      R/W  599   599INS
VMFUTL2205I BUILD4    K      R/W  505   505INS
VMFUTL2205I BUILD2    T      R/W  590   590INS
VMFUTL2205I BASE      U      R/W  2B2   2B2INS
VMFUTL2205I --------  A      R/W  191   191INS
VMFUTL2205I --------  B      R/W  5E5   MNT5E5
VMFUTL2205I --------  C      R/W  A22   A22TMP
VMFUTL2205I --------  D      R/W  51D   MNT51D
VMFUTL2205I --------  S      R/O  608   604RAC
VMFUTL2205I --------  Y/S    R/O  19E   19EMNT
VMFSET2760I VMFSETUP processing completed successfully
VMFREC2760I VMFREC processing started
VMFREC1852I Volume 1 of 1 of INS TAPE yynn
⋮
VMFREC2760I VMFREC processing completed successfully
VMFINT2603I Product installed
VMFINS2760I VMFINS processing completed successfully

Ready; T=20.25/21.69 16:48:02
```

In message VMFREC1852I, *yynn* is filled in with the RSU number.

2 Check the receive message log ($VMFREC $MSGLOG) for warning and error messages. If necessary, correct any problems before going on. For information about handling specific receive messages, see *z/VM System Messages and Codes*, or use online HELP.

vmfview install

A.1.3 Process Additional Service

1 Apply additional service.

The VMFAPPLY command is used to reapply service that was not contained on the refresh tape that was already installed for the component.

Applying service with preapplied, prebuilt service will reapply any reach-ahead service that may be on the system **or** indicate that there are no reach-ahead PTFs to be applied.

vmfapply ppf 6VMRAC10 {RACF | RACFSFS}

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

Messages VMFAPP2122E and VMFAPP2109R are displayed only if you have reach-ahead service that needs to be reapplied. If you receive these messages, enter **1** in reply to VMFAPP2109R to reapply the reach-ahead service (as shown in the example below).

```
VMFAPP2122E The set of PTFs in the Apply Status Table (6VMRAC10
        SRVAPPS) on the 2A2 (G) disk is not a subset of the
        PTFs in the highest level Apply Status Table on the
        2A6 (F) disk.  This is an inconsistent state.
VMFAPP2109R VMFAPPLY will automatically correct the problem identified
        by message 2122E by including the missing PTFs in the
        current Apply List.  Enter (1) to continue; (0) to quit.
```

1 Enter **1** for VMFAPPLY to reapply the reach-ahead service.

2 Check the apply message log ($VMFAPP $MSGLOG) for warning and error messages. If necessary, correct any problems before going on. For information about handling specific apply messages, see *z/VM System Messages and Codes*, or use online HELP.

vmfview apply

3 If necessary, rework **local modifications**.

The output from the VMFPSU command (which was run in an earlier step), *appid* **PSUPLAN** file, can be used to indicate what local service or mods are affected by the RSU. If a PTF is applied and it contains service to a part for

which you have a local modification, you will need to rework the local modification. Refer to *z/VM Service Guide*.

VMFPSU creates a **PSU $SELECT** file on the A-disk if you have any local modifications against RACF. This file has in it the local modifications affected by service, whether they required rework or just a rebuild. To ensure that your local modifications are rebuilt, append this file to the **TOP** of the 6VMRAC10 $SELECT file on the alternate APPLY disk.

If the **PSU $SELECT** file indicates that you have local modifications to HCPRPI, HCPRPD, HCPRPF, HCPRPG, HCPRPW, or HCPRWA that require rework, issue the following command before you rework the local modifications, to ensure that you have access to the latest copy of the RACF MACLIB:

vmfcopy racf maclib *fm-505* **= =** *fm-19E2* **(prodid 6VMRAC10%RACF olddate replace**

A.1.4 Build the RACF Base New Service Level and Place Into Production

To rebuild all objects that were flagged serviced on the RSU, affected by reach-ahead service that was reapplied and local modifications, continue with the instructions in 7.2.4, “Task 4. Update the Build Status Table” on page 77. This also leads you into the steps to place RACF into production.

Appendix B. RACF Local Modifications - Examples

All local modifications to serviceable parts must be entered into the software inventory to allow VMSES/E to track the changes and build them into the system. The following examples show how to put a local modification on to a RACF full part replacement assemble file or full part replacement part. For generic commands for all types of local modifications refer to *z/VM Service Guide*.

You can use the LOCALMOD and SERVICE BUILD commands, instead of these instructions, to put a local modification on to RACF. Refer to the Appendix "Apply or Rework a Local Modification" in the *z/VM: Guide for Automated Installation and Service*. You will still need to refer to the instructions below for any information on changing the actual content of the file being modified.

B.1 Assemble Full Part Replacement - Example

1 Establish the 6VMRAC10's minidisk access order.

VMFSETUP 6VMRAC10 {RACF | RACFSFS}

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

2 Copy the assemble file to the 2C2 (E-disk). If you are following these procedures after installing, it is possible that this file already exists on the LOCALSAM 2C2 disk. If you have a copy of the file on the 2C2 disk, use this copy of the file to make your new local modification.

3 Make your local modification changes to the copy on your LOCALSAM 2C2 disk.

4 Issue the assemble command for the file:

vmfhlasm *fn* **6VMRAC10 {RACF | RACFSFS}**

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

Notes:

1. Other options are available for the assemble commands. Consult *z/VM: VMSES/E Introduction and Reference* for additional information. You should use the VMFHLASM assemble exec supplied by VMSES/E.
2. If the assemble function is successful, the file *fn* TXT00000 is placed on the A-disk.

5 Copy the *fn* TXT00000 file from the A-disk to the 2C2 E-disk as *fn* TXTL*nnnn*.

copyfile *fn* **txt00000 a = txtl***nnnn* **e**

Note: TXTL is a required filetype for local modified text. *nnnn* is a user-defined number assigned to this fix, usually starting with 0001.

6 Erase the TXT00000 file from your A-disk.

erase *fn* **txt00000 a**

7 Rename the assemble file on the 2C2 E-disk as *fn* ASML*nnnn* E.

rename *fn* **assemble** *2c2-fm* **= asml***nnnn 2c2-fm*

8 Update the VVT tables for both the TXT and ASM files by issuing the following VMFSIM against both the text and the assemble files:

vmfsim logmod 6VMRAC10 vvtlcl e tdata :mod lcl*nnnn* **:part** *fn* **txt**
vmfsim logmod 6VMRAC10 vvtlcl e tdata :mod lcl*nnnn* **:part** *fn* **asm**

9 Build your new local modification on the test build disk by issuing the following command.

vmfbld ppf 6VMRAC10 {RACF | **RACFSFS}** *blist memname* **(all**

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

B.2 Full Part Replacement (Not Assemble) - Example

The following example can be used for putting a local modification on to a RACF part that is serviced by full part replacement. The commands have substitution values that you need to supply. The instructions that pointed you to this example should have the substitution values for that particular local modification.

1 Establish the 6VMRAC10's minidisk access order.

access 590 t
vmfsetup 6VMRAC10 {RACF | RACFSFS}

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

2 Copy the file to the 2C2 (E-disk) using the local modification identifier along with the file type abbreviation of the file type.

copyfile *fn ft fm* **=** *ft-abbrv***L***nnnn* **e**

Note: *nnnn* is a user-defined number assigned to this fix, usually starting with 0001.

3 Make your local modification changes to the copy on your LOCALSAM 2C2 disk.

4 Update the VVT table for the part or file by issuing the following VMFSIM against the assemble file:

vmfsim logmod 6VMRAC10 vvtlcl e tdata :mod lcl*nnnn* **:part** *fn ft-abbrv*

5 Build your new local modification on the test build disk by issuing the following command. (If the part appears in more than one build list then you need to issue the VMFBLD command for each build list.)

vmfbld ppf 6VMRAC10 {RACF | RACFSFS } *blist memname* **(all**

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

B.3 Local Modification to Full Part Replacement Text Files and Possible Build List Update

During customization of RACF you might have to modify TEXT files that are serviced as full part replacement, using your created ASSEMBLE file.

Follow the instructions here to create and build the new TEXT file. You should have been given any substitution command values in the instructions that pointed you to this section.

1 Establish the 6VMRAC10's minidisk order.

access 590 t
vmfsetup 6VMRAC10 {RACF | RACFSFS}

2 If you are deleting a part from a build list continue with step 8 on page 101.

3 Create your assemble file on the 2C2 (E) disk.

4 Issue the assemble command for the file:

vmfhlasm *fn* **6VMRAC10 {RACF | RACFSFS} ($select outmode** *2c2-fm*

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

Notes:

1. Other options are available for the assemble commands. Consult *z/VM: VMSES/E Introduction and Reference* for additional information. You should use the VMFHLASM assemble exec supplied by VMSES/E.
2. If the assemble function is successful, the file *fn* TXT00000 will be placed on the LOCALSAM 2C2 (E) disk.

5 Rename the *fn* TXT00000 file on the 2C2 E-disk to *fn* TXTL*nnnn*.

rename *fn* **txt00000** *2c2-fm fn* **txtl***nnnn 2c2-fm*

Note: TXTL is a required filetype for local modified text. *nnnn* is a user-defined number assigned to this fix.

6 Update the VVT tables for the TXT file by issuing the following VMFSIM command against the text file:

vmfsim logmod 6VMRAC10 vvtlcl *2c2-fm* **tdata :mod lcl***nnnn* **:part** *fn* **txt**

7 If you are not adding to or deleting from a build list then continue with step 13 on page 102.

8 To add objects to or take objects from a build list you need to get the highest level of the build list used to build the library that the part resides in. You need this to determine the file type to use in the next step.

vmfsim getlvl 6VMRAC10 {RACF | RACFSFS} tdata :part *blist* **exc (history**

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

If the response **does not contain** the :PTF tag or :MOD tag, there is no service to the build list (you will see **exc00000 base-filetype**). In this case use **exec** in the next step as the file type.

If the response **contains** the :PTF tag or :MOD tag, there is a local modification or IBM service against the build list. VMSES/E takes a local modification as the highest level of a part followed by the PTF level as the next highest. If there was a local modification, the file type to use in the next command id **exc***modid* (where *modid* is the Lmmmm part of LCLmmmm in the VMFSIM output). If there was no local modification, the file type to use in the next command id **exc**-*ptfnumber* (where *-ptfnumber* is filled in with the real PTF number).

9 Copy the highest level of the build list to the 2C2 (E-disk) local disk.

copyfile *blist ft fm* **= excl***nnnn 2c2-fm*

ft is the file type from the previous step.

nnnn is a free local modification number, for example 0002.

10 Do this step if you need to add a new command part to a build list. Add the following statements to the new copy of the build list, on the 2C2 disk, at the end of the build list.

The following is an example of what you would add into a TXTLIB build list:

```
:OBJNAME. memname.
:OPTIONS. NOGETLVL
:PARTID. memname TEXT
:EOBJNAME.
*
```

Where *memname* is the file name of your new command TEXT file.

The following is an example of what you would add into a LOADLIB build list:

```
:OBJNAME. memname LEPARMS RENT REUS LET NCAL XREF SIZE 100K,80K
:OPTIONS. NOGETLVL
:PARTID.  memname TEXT
:EOBJNAME.
*
```

Where *memname* is the file name of your new command TEXT file.

11 If you need to remove an object from the build list(s), for example ICHDEX01, comment out (put an asterisk in front of each line) the following lines from the *blist* build list on the 2C2 (E-disk). Otherwise continue with the next step.

```
:OBJNAME. ICHDEX01 LEPARMS RENT REUS LET NCAL XREF DCBS SIZE 100K,80K
:BLDREQ. RPIBLOBJ.ICHDEX01
:OPTIONS. CONCAT SYSLIB RACFOBJ
:OPTIONS. INCLUDE RACFOBJ(ICHDEX01)
:OPTIONS. ENTRY ICHDEX01
:EOBJNAME.
```

12 Update the local VVT table for the modified build list.

vmfsim logmod 6VMRAC10 vvtlcl e tdata :mod lcl*nnnn* **:part** *blist* **exc**

13 Build your new local modification on the test build disk.

a If you are deleting a part from a build list, for example ICHRCX02, do this step.

vmfbld ppf 6VMRAC10 {RACF | RACFSFS} *blist* **(all**

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

b If you are local modifying TEXT file, do this step.

vmfbld ppf 6VMRAC10 {RACF | RACFSFS} (serviced

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

c If you are adding to a build list, do this step.

vmfbld ppf 6VMRAC10 {RACF | RACFSFS} *blist memname* **(all**

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

14 Place the new local modification into production.

Note: In order to do this step you need to shutdown RACFVM server machine and bring up the RACMAINT server machine in order to get write access to the production disk.

link RACFVM 305 305 MR
acc 505 e
acc 305 f
vmfcopy * * e = = f (prodid 6VMRAC10%RACF olddate replace

The use of RACF in the prodid parameter is correct.

15 Re-IPL each RACF service machine.

B.4 Local Modification to Full Part Assemble and Text Files and Possible Build List Update

During customization of RACF you might have to modify ASSEMBLE files and corresponding TEXT files that are serviced as full part replacement.

Use the following instructions to create and build the new part. You should have been given any substitution command values in the instructions that pointed you to this section.

1 Establish the 6VMRAC10's minidisk order.

access 590 t
vmfsetup 6VMRAC10 {RACF | RACFSFS}

2 If you are deleting a part from a build list continue with step 10 on page 105.

3 Copy the assemble file to the 2C2 disk (E-disk). Make sure you use the version of the assemble file that is on the production build disk or the test build disk.

4 Make your local modification to the copy of the ASSEMBLE file on your LOCALSAM 2C2 disk.

5 Issue the assemble command for the file:

vmfhlasm *fn* **6VMRAC10 {RACF | RACFSFS} ($select outmode** *2c2-fm*

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

Notes:

1. Other options are available for the assemble commands. Consult *z/VM: VMSES/E Introduction and Reference* for additional information. You should use the VMFHLASM assemble exec supplied by VMSES/E.
2. If the assemble function is successful, the file *fn* TXT00000 will be placed on the LOCALSAM 2C2 (E) disk.

6 Rename the *fn* TXT00000 file on the 2C2 E-disk to *fn* TXTL*nnnn*.

rename *fn* **txt00000** *2c2-fm fn* **txtl***nnnn 2c2-fm*

Note: TXTL is a required filetype for local modified text. *nnnn* is a user-defined number assigned to this fix.

7 Rename the assemble file on the 2C2 E-disk as *fn* ASML*nnnn*.

rename *fn* **assemble** *2c2-fm fn* **asml***nnnn 2c2-fm*

8 Update the VVT tables for both the TXT and ASM files by issuing the following VMFSIM commands against both the text and the assemble files:

vmfsim logmod 6VMRAC10 vvtlcl *2c2-fm* **tdata :mod lcl***nnnn* **:part** *fn* **txt**
vmfsim logmod 6VMRAC10 vvtlcl *2c2-fm* **tdata :mod lcl***nnnn* **:part** *fn* **asm**

9 If you are not adding to or deleting from a build list then continue with step 15 on page 106.

10 To add objects to or take objects from a build list you need to get the highest level of the build list used to build the library that the part resides in. You need this to determine the file type to use in the next step.

vmfsim getlvl 6VMRAC10 {RACF | RACFSFS} tdata :part *blist* **exc (history**

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

If the response **does not contain** the :PTF tag or :MOD tag, there is no service to the build list (you will see **exc00000 base-filetype**). In this case use **exec** in the next step as the file type.

If the response **contains** the :PTF tag or :MOD tag, there is a local modification or IBM service against the build list. VMSES/E takes a local modification as the highest level of a part followed by the PTF level as the next highest. If there was a local modification, the file type to use in the next command id **exc***modid* (where *modid* is the Lmmmm part of LCLmmmm in the VMFSIM output). If there was no local modification, the file type to use in the next command id **exc**-*ptfnumber* (where *-ptfnumber* is filled in with the real PTF number).

11 Copy the highest level of the build list to the 2C2 (E-disk) local disk.

copyfile *blist ft fm* **= excl***nnnn 2c2-fm*

ft is the file type from the previous step.

nnnn is a free local modification number, for example 0002.

12 Do this step if you need to add a new command part to a build list. Add the following statements to the new copy of the build list, on the 2C2 disk, at the end of the build list.

The following is an example of what you would add into a TXTLIB build list:

```
:OBJNAME. memname.
:OPTIONS. NOGETLVL
:PARTID. memname TEXT
:EOBJNAME.
*
```

Where *memname* is the file name of your new command TEXT file.

The following is an example of what you would add into a LOADLIB build list:

```
:OBJNAME. memname LEPARMS RENT REUS LET NCAL XREF SIZE 100K,80K
:OPTIONS. NOGETLVL
:PARTID.  memname TEXT
:EOBJNAME.
*
```

Where *memname* is the file name of your new command TEXT file.

13 If you need to remove an object from the build list(s), for example ICHRCX02, comment out (put an asterisk in front of each line) the following lines from the *blist* build list on the 2C2 (E-disk). Otherwise continue with the next step.

```
:OBJNAME. ICHRCX02 LEPARMS RENT REUS LET NCAL XREF DCBS SIZE 100K,80K
:OPTIONS. CONCAT SYSLIB RACFOBJ
:PARTID. ICHRCX02 TXT
:OPTIONS. ENTRY ICHRCX02
:EOBJNAME.
```

14 Update the local VVT table for the modified build list.

vmfsim logmod 6VMRAC10 vvtlcl e tdata :mod lcl*nnnn* **:part** *blist* **exc**

15 Build your new local modification on the test build disk.

a If you are deleting a part from a build list, for example ICHRCX02, do this step.

vmfbld ppf 6VMRAC10 {RACF | RACFSFS} *blist* **(all**

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

b If you are local modifying the ASSEMBLE and TEXT file, do this step.

vmfbld ppf 6VMRAC10 {RACF | RACFSFS} (serviced

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

C If you are adding to a build list, do this step.

vmfbld ppf 6VMRAC10 {RACF | RACFSFS} *blist memname* **(all**

Use:	if installed:
RACF	on minidisks
RACFSFS	in SFS directories

16 Place the new local modification into production.

Note: In order to do this step you need to shutdown RACFVM server machine and bring up the RACMAINT server machine in order to get write access to the production disk.

link RACFVM 305 305 MR
acc 505 e
acc 305 f
vmfcopy * * e = = f (prodid 6VMRAC10%RACF olddate replace

The use of RACF in the prodid parameter is correct.

17 Re-IPL each RACF service machine.

Appendix C. Starting, Stopping, and Disabling RACF

This appendix describes how to start, stop (temporarily suspend), reactivate, and disable RACF.

C.1 Starting and Restarting RACF

To start or restart a RACF service machine, for example RACFVM, you can use **one** of the following methods:

- Log on to RACFVM and enter:

  ```
  CP IPL 490
  RACSTART
  ```

- From the primary system operator, enter:

  ```
  FORCE RACFVM
  XAUTOLOG RACFVM
  ```

- From a user defined as a secondary console of RACFVM, enter:

  ```
  SEND RACFVM CP IPL 490
  ```

  Note: It is not necessary to enter RACSTART because RACFVM is running disconnected; the RACSTART is performed automatically from within RACFVM's PROFILE EXEC.

C.2 Temporarily Suspending and Reactivating RACF

Use the SETRACF command to temporarily suspend (deactivate) or reactivate RACF.

Attention

Use care when issuing the SETRACF command to deactivate RACF. When you deactivate RACF, access control reverts to CP. CP uses the information in the CP directory to control a user's access to the system (using the user's password) and to minidisks (using CP links). The information in the CP directory is probably not current with the equivalent information in the RACF database.

For example, if your installation changes a user's access authority to a minidisk from CONTROL to READ in the RACF data base, this change is not reflected automatically in the CP directory.

If you find it necessary to deactivate RACF, you should not allow general users to log on to the system while RACF is inactive.

SETRACF is a CMS command, not a RACF command; therefore you cannot enter SETRACF using RAC or during a RACF command session.

You can issue the SETRACF command only from a RACF service machine. The RACF service machine can, however run disconnected, thereby allowing a secondary console to issue this command.

By default, RACF sets up the OPERATOR as the secondary console for the RACF service machine; the OPERATOR can issue the command to deactivate RACF. For example,

```
SEND RACFVM SETRACF INACTIVE
```

If you issue SETRACF for any RACF service machine in a multiple service machine environment, it applies to all service machines.

For additional information about SETRACF, see *z/VM: RACF Security Server Command Language Reference*.

C.2.1 Temporarily Suspending RACF

To suspend RACF, enter:

```
SETRACF INACTIVE
```

The operator receives the following messages:

```
HCPRPD001I REQUEST TO SET RACF INACTIVE MADE BY RACFVM
HCPRPD001I REQUEST TO SET RACF INACTIVE MADE BY RACFVM
HCPRPD001I REQUEST TO SET RACF INACTIVE MADE BY RACFVM
HCPRPD002A REPLY YES TO ALLOW DEACTIVATION - ANYTHING ELSE WILL CANCEL REQUEST
```

The operator must respond `YES`.

C.2.2 Reactivating RACF

To reactivate RACF when it has been suspended, enter:

```
SETRACF ACTIVE
```

C.3 Disabling RACF On Your VM System

You can use the following procedure to disable RACF:

__ Step 1. From OPERATOR user ID you need to FORCE RACFVM and XAUTOLOG RACMAINT. Need to do this so that PUT2PROD can run in the next step.

__ Step 2. Regenerate the CP nucleus to replace the RACF modules with the VM modules: `HCPRWA`, `HCPRPI`, `HCPRPF`, `HCPRPG`, `HCPRPD`, and `HCPRPW`. To do this the the RACF local modification to CP needs to be removed. RACF also needs to be disabled. To accomplish this you need to issue the following commands from the MAINT user ID:

```
service racf disable
put2prod
```

__ Step 3. Remove `XAUTOLOG` statements for all RACF service machines from the AUTOLOG1 profile.

__ Step 4. Move the functions from AUTOLOG2 back to AUTOLOG1.

__ Step 5. Remove user LINKs to the RACFVM disks.

__ Step 6. Modify DirMaint:

a. Comment out the CONFIG DATADVH item `ESM_PASSWORD_AUTHENTICATION_EXIT`.

b. Change the CONFIG DATADVH items `PW_WARN_MODE` and `PW_LOCK_MODE` to `AUTOMATIC`, if appropriate for your installation.

c. Comment out the CONFIG DATADVH item `ESM_LOG_RECORDING_EXIT`.

d. If using the sample RACF override CONFIGRC DATADVH file, RENAME it to CONFIGRC SAMPDVH. See the *z/VM Directory Maintenance Facility Tailoring and Administration Guide* for more information.

For these changes to take effect, either IPL DIRMAINT or enter the DIRM RLDDATA command.

__ Step 7. Remove RACF files from the 19E system disk, ISPF disk and GCS disk. You can use the VMFERASE command to remove those files if you used VMFCOPY to place the files on those disks. For example:

```
ACC 19E Z
VMFERASE PROD 6VMRAC10%RACF FROM Z
```

__ Step 8. Modify SFS file pool servers.

If you are using RACF to protect SFS resources, disable RACF support by changing the *server_id* DMSPARMS file on each SFS file pool server to specify `NOESECURITY` instead of `ESECURITY`.

__ Step 9. Modify BFS file pool servers.

If you are using RACF to protect BFS resources, disable RACF support by doing the following:

a. Change the *server_id* DMSPARMS file on each BFS file pool server to specify `NOESECURITY` instead of `ESECURITY`.

b. Delete the file ESMLIB CSLLIB from each BFS file pool server. This file probably resides on the A-disk of the server.

c. In the PROFILE EXEC of each BFS file pool server, remove the `RTNLOAD DMSPERM` statement.

__ Step 10. Modify RACROUTE applications.

If you have applications or other program products which use the RACROUTE interface, you might have to change them. If you are replacing RACF with an equivalent security product, that product might or might not support the RACROUTE interface.

To assist you in determining if any applications are using the RACROUTE interface, you can display which user IDs are authorized by RACF to issue RACROUTE requests. To do this, use the RLIST command to display the access list for the ICHCONN profile in the FACILITY class:

```
RLIST FACILITY ICHCONN AUTH
```

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other 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.

Licenses 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
RACF Development
Department G15G, Mail Station P388
Poughkeepsie, New York 12601-5400
U.S.A.

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 the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at

www.ibm.com/legal/copytrade.shtml

Adobe, the Adobe logo, PostScript and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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

Index

S

T

U

V

Reader's Comments

IBM® RACF Security Server for z/VM, function level 610

You may use this form or the VM Feedback page (Contact z/VM) on the z/VM Web site at:

www.ibm.com/eserver/zseries/zvm/forms/

to comment about this document, its organization, or subject matter.

Please understand that your feedback is of importance to IBM, but IBM makes no promises to always provide a response to your feedback.

For each of the topics below please indicate your satisfaction level by circling your choice from the rating scale. If a statement does not apply, please circle N.

RATING SCALE

very satisfied				very dissatisfied	not applicable
1	2	3	4	5	N

	Satisfaction					
Ease of product installation	1	2	3	4	5	N
Time required to install the product	1	2	3	4	5	N
Contents of program directory	1	2	3	4	5	N
Readability and organization of program directory tasks	1	2	3	4	5	N
Necessity of all installation tasks	1	2	3	4	5	N
Accuracy of the definition of the installation tasks	1	2	3	4	5	N
Technical level of the installation tasks	1	2	3	4	5	N
Installation verification procedure	1	2	3	4	5	N
Ease of customizing the product	1	2	3	4	5	N
Ease of migrating the product from a previous release	1	2	3	4	5	N
Ease of putting the system into production after installation	1	2	3	4	5	N
Ease of installing service	1	2	3	4	5	N

- If you ordered this product as part of a package, then what type of package was ordered?
  - □ System Delivery Offering (SDO)
  - □ Other - Please specify type: _____

- Is this the first time your organization has installed this product?
  - □ Yes
  - □ No
- Were the people who did the installation experienced with the installation of VM products using VMSES/E?
  - □ Yes

    How many years of experience do they have? _____
  - □ No
- How long did it take to install this product? _____
- If you have any comments to make about your ratings above, or any other aspect of the product installation, please list them below:

  _____

  _____

  _____

  _____

  _____

  _____

  _____

  _____

Please provide the following contact information:

_____

Name and Job Title

_____

Organization

_____

_____

Address

_____

Telephone

Thank you for your participation.

Please send the completed form to the following address, or give to your IBM representative who will forward it to the RACF Security Server for z/VM Development group:

IBM Corporation
RACF Development
Department G15G, Mail Station P388
2455 South Road
Poughkeepsie, New York 12601-5400
USA

Program Number: 5741-A07

Printed in USA

GI11-4325-00