Program Directory for

RACF Security Server for z/VM

function level 720

Program Number 5741-A09

for Use with
z/VM version 7 release 2

Document Date: September 2020

GI13-4364-01

Attention

Before using this information and the product it supports, be sure to read the general information under “Notices” on page 57.

This program directory, dated September 2020, applies to IBM® RACF® Security Server for z/VM®, function level 720, Program Number 5741-A09.

A link for a reader's comments form 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

1.0 Introduction . . . 1
1.1 Program Description . . . 1

2.0 Program Materials . . . 3
2.1 Basic Machine-Readable Material . . . 3
2.2 Optional Machine-Readable Material . . . 3
2.3 Program Publications . . . 3
2.3.1 Basic Program Publications . . . 3
2.3.2 Base Program Publications . . . 4
2.3.3 Softcopy Publications . . . 4
2.4 Program Source Materials . . . 4
2.5 Publications Useful During Installation and Service . . . 5

3.0 Program Support . . . 6
3.1 Preventive Service Planning . . . 6
3.2 Statement of Support Procedures . . . 6

4.0 Program and Service Level Information . . . 8
4.1 Program Level Information . . . 8
4.2 Service Level Information . . . 8
4.3 Cumulative Service . . . 8
4.4 How to Determine Your RSU Service Level . . . 9

5.0 Installation Requirements and Considerations . . . 10
5.1 Hardware Requirements . . . 10
5.2 Program Considerations . . . 10
5.2.1 Operating System Requirements . . . 10
5.2.2 Other Program Product Requirements . . . 10
5.2.2.1 General . . . 10
5.2.2.2 Dual Registration . . . 11
5.2.3 Sharing a RACF Database . . . 11
5.2.4 Restrictions When Using FBA Devices . . . 12
5.2.5 RACF in conjunction with System Migration . . . 12
5.2.6 VMSES/E Program Installation and Service Considerations . . . 13
5.3 DASD Storage and User ID Requirements . . . 13
5.4 ICHDEX01 Exit and Masked Passwords Considerations . . . 17

6.0 Installation Instructions . . . 18
6.1 Overview of the VMSES/E Installation Process . . . 19
6.2 Overview of the RACF Installation Steps . . . 19
6.3 Task 1. Review Resources for Installing RACF . . . 20
6.3.1 General RACF User ID Information . . . 21

6.3.2 Sharing a RACF Database Information . . . 22
6.4 Task 2. Upgrade the Database Templates . . . 23
6.5 Task 3. Prepare to Update RACF with Existing CP Directory Data . . . 27
6.5.1 Run RPIDIRCT to Create the RPIDIRCT SYSUT1 File . . . 28
6.6 Task 4. Customize the Processing of SMF Records (Optional) . . . 29
6.7 Task 5. Customize RACF Within CP (Optional) . . . 30
6.8 Task 6. Install the CP Part of RACF . . . 31
6.9 Task 7. Change RACF Database Names If Sharing with z/OS System . . . 32
6.10 Task 8. IPL the CP System with RACF . . . 33
6.11 Task 9. Update the RACF Database with Existing CP Directory Information . . . 34
6.11.1 Initialize the RACF Database (If You Are Not Sharing an Existing Database) . . . 35
6.11.1.1 Logging On to the IBMUSER User ID . . . 35
6.11.1.2 Building the RACF Database . . . 36
6.11.1.3 Defining the Security Administrator and Maintenance User IDs. . . . 37
6.11.2 Update the RACF Database (If You Are Sharing an Existing Database) . . . 38
6.12 Task 10. Create the Global Access Table (Optional) . . . 39
6.13 Task 11. Set RACF Options . . . 39
6.14 Task 12. Determine Audit and Control Options for VM Events (Optional) . . . 40
6.15 Task 13. Set Up the DirMaint-RACF Connector if DirMaint is Installed (Optional) . . . 41
6.16 Task 14. Place RACF Into Production . . . 42
6.16.1 Copy RACF Files Into Production . . . 42

7.0 Service Instructions . . . 45
7.1 Servicing RACF . . . 45

Appendix A. Set up the RACF ISPF Panels . . . 46
A.1 Modify the ISPF Files For Use With PDF . . . 46
A.1.1 Step 1 - Modify the ISPF EXEC Filedefs . . . 46
A.1.2 Step 2 - Modify the ISPF EXEC ISPDCS Line . . . 48
A.1.3 Step 3 - Modify RACF ISPF-Supplied Files . . . 48
A.2 Modify the ISPF Files for use with non-PDF . . . 49
A.2.1 Step 1 - Modify the ISPSTART EXEC Filedefs . . . 49
A.2.2 Step 2 - Modify the ISPF EXEC ISPDCS Line . . . 50
A.2.3 Step 3 - Modify RACF ISPF-Supplied Files . . . 50
A.2.3.1 Update ICHSFSIN EXEC . . . 50
A.2.3.2 Update RACF EXEC . . . 51
A.3 Modify the ISPF Primary Option Panel . . . 53
A.4 Dual Registration Users Only . . . 53
A.4.1 Set Defaults in PROFILE . . . 53
A.4.2 Verify directory entries . . . 54
A.5 Invoke the RACF ISPF Panels . . . 54
A.6 Full Part Replacement (Not Assemble) - Example . . . 54

Notices . . . 57
Privacy Policy Consideration . . . 58
Trademarks . . . 58

Index 60

Reader's Comments 61

Figures

1. Basic Material: Informal Documentation 3
2. Basic Material: Unlicensed Publications 4
3. Program Publications: New Editions 4
4. Publications Useful During Installation / Service on z/VM V7.2 5
5. PSP Upgrade and Subset ID 6
6. Component IDs 7
7. DASD Storage Requirements for Target Minidisks 14
8. Sample Filedefs for the ISPF EXEC for Systems with PDF 47
9. Sample Filedefs for the ISPSTART EXEC for Systems without PDF 49
10. Changes for RACF EXEC INIT Routine for Systems without PDF 52

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 18 provides detailed installation instructions for RACF.
- 7.0, “Service Instructions” on page 45 provides servicing instructions for RACF.
- Appendix A, “Set up the RACF ISPF Panels” on page 46 provides steps on how to set up the RACF ISPF Panels

Before enabling 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 720 is 5741-A09.

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 720, to obtain a license for it.** Refer to the z/VM version 7 release 2 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

Figure 1 identifies the informal shipped documentation for RACF. One copy of this publication is included with your RACF order.

Figure 1. Basic Material: Informal Documentation

Publication Title	Form Number
Memo to Users IBM RACF Security Server for z/VM, function level 720	GI13-4371

The following publication is part of your order for RACF but it is only available as softcopy. Refer to 2.3.3, "Softcopy Publications" on page 4 for the World Wide Web URLs that this program directory can be found at.

Figure 2. Basic Material: Unlicensed Publications

Publication Title	**Form Number**
RACF Security Server for z/VM Program Directory	GI13-4364

2.3.2 Base Program Publications

Figure 3 identifies the program publications available for RACF.

Figure 3. Program Publications: New Editions

Publication Title	**Form Number**
z/VM: RACF Security Server Command Language Reference	SC24-6308
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	SC24-6309
z/VM: RACF Security Server Messages and Codes	GC24-6217
z/VM: RACF Security Server Diagnosis Guide	GC24-6307

2.3.3 Softcopy Publications

The RACF publications are available as part of RACF library in the IBM Knowledge Center web site:

http://www.ibm.com/support/knowledgecenter/SSB27U

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.vm.ibm.com/library/

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 4 may be useful during the installation of RACF. To order copies, contact your IBM representative.

Figure 4. Publications Useful During Installation / Service on z/VM V7.2

Publication Title	Form Number
z/VM: VMSES/E Introduction and Reference	GC24-6336
z/VM: Installation Guide	GC24-6292
z/VM: Service Guide	GC24-6325
z/VM: CP Planning and Administration	SC24-6271
z/VM: CMS Commands and Utilities Reference	SC24-6268
z/VM: CMS File Pool Planning, Administration, and Operation	SC24-6261
z/VM: Other Components Messages and Codes	GC24-6207
z/VM: CMS and REXX/VM Messages and Codes	GC24-6255
z/VM: CP Messages and Codes	GC24-6270
z/VM: Running Guest Operating Systems	SC24-6321
z/VM: System Operation	SC24-6326

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 5. PSP Upgrade and Subset ID

Retain			
COMPID	**Release**	**Upgrade**	**Subset**
576700201	720	RACFVM720	RACF720
576700201	720	RACFVM720	yynnRSU

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

www.vm.ibm.com/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 V7.2, you are entitled to support under the basic warranty for z/VM V7.2. Also, note that the Software Subscription and Support for the RACF Security Server for z/VM is *automatically* added to your order. This provides IBM Z® 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 6 identifies the component ID (COMPID), Retain® Release and Field Engineering Service Number (FESN) for RACF.

Figure 6. Component IDs

Retain			
COMPID	**Release**	**Component Name**	**FESN**
576700201	720	RACF FL720	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 have been incorporated into this release:

VM65082 VM65192 VM65214 VM65222 VM65247 VM65294 VM65296 VM65320
VM65493 VM65498 VM65532 VM65542 VM65553 VM65573 VM65580 VM65609
VM65688 VM65719 VM65742 VM65759 VM65767 VM65773 VM65779 VM65792
VM65795 VM65808 VM65840 VM65857 VM65923 VM65930 VM65931 VM66123
VM66152 VM66278 VM66286 VM66338

4.2 Service Level Information

Check the RACFVM720 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 720, 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 V7 stacked RSU, which would include RACF, can be obtained by ordering PTF UM97720.

Check the PSP bucket upgrade RACFVM720 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.vm.ibm.com/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.

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. This is a SAMPLE only. The RSU service level may NOT match what you see. The VMFSRV1225I message indicates the RSU service level.

```
VMFSRV2760I SERVICE processing started
VMFSRV1225I RACF (7VMRAC20%RACF) status:
VMFSRV1225I    Service Level     RSU-2001
VMFSRV1225I    Production Level  SYSTEM1.RSU-2001
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. You must be logged on to a user ID with access to the VMSES/E programs and the system and product inventory disks. MAINT720 is recommended.

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 720, will operate on any processor supported by:

- z/VM version 7 release 2

On z/VM the minidisks for the RACF database (defined at virtual addresses 200 and 300) can reside on any DASD supported by z/VM version 7 release 2.

Note: Sharing the RACF database, whether in an SSI or not, requires ECKD.

For the most current information on devices supported by z/VM version 7 release 2, refer to *z/VM General Information* manual. For more information on using FBA DASD devices, see 5.2.4, “Restrictions When Using FBA Devices” on page 12.

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 7 release 2

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 is required by z/VM version 7 and is pre-installed on the z/VM system deliverables.

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. HLASM is no longer required to assemble HCPRWA and

HCPRWAC. The Assembler XF (that is is shipped as part of z/VM CMS) can be used for those two RACF CP parts.

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 720

5.2.3 Sharing a RACF Database

A RACF database can be shared with another operating system, either z/OS® or z/VM. In general a RACF database can be shared with a system that has another level of RACF installed.

When RACF is installed in a single-member or multiple-member z/VM single system image (SSI) environment, it is mandatory that the RACF database is configured as being shared.

A RACF database residing on FBA (SCSI) DASD cannot be shared.

To ensure integrity of the RACF database, careful consideration needs to be given if the database is to be shared.

- If the RACF database is to be shared between multiple RACF servers on the same real system, then you must configure the database minidisks to use virtual reserve/release.
- If the RACF database is to be shared between single RACF servers on different real systems, then you must configure the database DASD to use real reserve/release.
- If the RACF database is to be shared between multiple RACF servers on the same real system and RACF servers on different real systems, then you must configure the database DASD to use concurrent virtual and real reserve/release.

  Note: Concurrent virtual and real reserve/release must always be used for the RACF database DASD when RACF is installed in an SSI.

See *z/VM: RACF Security Server System Programmer's Guide* for more information on sharing a RACF database and *z/VM: CP Planning and Administration* for information on DASD Sharing.

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.

For z/VM single system image (SSI) environment, there are examples of RACF CP user directory entries in the section "Sharing RACF Databases in a z/VM Single System Image Cluster" in the *z/VM: RACF Security Server System Programmer's Guide*.

During initialization if the database is not configured to be 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.

5.2.4 Restrictions When Using FBA Devices

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

- RACF databases *cannot* be shared on FBA device types.
- The number of RACF databases is limited to one primary and one backup.
- The multiple RACF service machines capability cannot be used.
- For the most current information on FBA DASD devices supported by z/VM, on which the RACF database can reside, refer to the *z/VM: General Information* manual.

5.2.5 RACF in conjunction with System Migration

When you use the upgrade installation procedure documented in the *z/VM: Installation Guide* to migrate RACF from z/VM V6.4 or z/VM V7.1 to z/VM V7.2, the customizable files will be migrated to z/VM V7.2. As part of the upgrade, you will be told to rework your changes.

Note: If you created your own RACF exit programs and placed them on the RACF install user ID's 2C2 disk or SFS directory, and did not have instructions that placed the part in the RACF service version vector table (VVT), you may need to move these parts to the new 2C2 disk or SFS directory. You may need to force a build by following the instructions in the *z/VM: RACF Security Server System Programmer's Guide*, section 'Build or Link-Edit a Library' in order to include them in your library.

The size of the 7VMRAC20 490 and the RACF 590 disks are now 70 cylinders and are RECOMPed to 63 cylinders.

5.2.6 VMSES/E Program Installation and Service Considerations

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

- RACF Security Server for z/VM is pre-installed on the z/VM version 7 release 2 deliverables.
- With the packaging changes introduced with z/VM version 6 release 3 to provide support for a z/VM single system image (SSI), note that **all RACF Security Server service activity now must be performed using user ID MAINT*vrm* (for example MAINT720).**
- VMSES/E is required to install and service this product.
- If you modify or eliminate any of the IBM-supplied user IDs, minidisk addresses or SFS directory names that are associated with RACF Security Server for z/VM, you **must** create an appropriate PPF override for the **SERVP2P $PPF** file. You also must use the **VMFUPDAT SYSSUF** command to update the VM SYSSUF Software Inventory file, so that your PPF override for SERVP2P PPF is used for automated service processing. For more information about PPF overrides, see the *z/VM: VMSES/E Introduction and Reference*.
- If multiple users install and maintain licensed products on your system, there may be a problem getting the necessary access to MAINT720'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.
- RSUs will be supplied as necessary. Service between RSUs can be obtained through CORrective service.

5.3 DASD Storage and User ID Requirements

Figure 7 on page 14 lists the user IDs and minidisks that are used to install and service RACF.

Important Installation Notes:

- All user IDs 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.
- The RACF Security Server for z/VM user ID that owns the service resources (7VMRAC20), and the IBMUSER and SYSADMIN virtual

machines are defined by single-configuration virtual machine definitions. All other RACF server virtual machines are defined by multiconfiguration virtual machine definitions. See *z/VM: CP Planning and Administration* for information on multiconfiguration and single-configuration virtual machine definitions.

- Figure 7 shows minimum space allocations. Depending on the requirements of your system, you might have to increase these sizes.

Figure 7 (Page 1 of 2). 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**
7VMRAC20	2B2	3390	85	122 400	15 300	Contains all the base code shipped with RACF **VMPSFS:7VMRAC20.RACF.OBJECT**
7VMRAC20	2C2	3390	9	12 960	1620	Contains customization files. This disk can also be used for local modifications. **VMPSFS:7VMRAC20.RACF.SAMPLE**
7VMRAC20	2D2	3390	70	100 800	12 600	Contains serviced files **VMPSFS:7VMRAC20.RACF.DELTA**
7VMRAC20	2A6	3390	9	12 960	1620	Contains AUX files and software inventory tables that represent the test service level of RACF **VMPSFS:7VMRAC20.RACF.APPLYALT**
7VMRAC20	2A2	3390	9	12 960	1620	Contains AUX files and software inventory tables that represent the service level of RACF that is currently in production. **VMPSFS:7VMRAC20.RACF.APPLYPROD**
7VMRAC20	29E	3390	10	14400	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.
7VMRAC20	590	3390	70	100 800	NOSFS	Test CST/CMS system build disk.
7VMRAC20	505	3390	41	59 040	NOSFS	Test server code build disk.
7VMRAC20	599	3390	31	44 640	NOSFS	RACF ISPF Panels
7VMRAC20	651	3390	1	14 40	NOSFS	Common system parts test build disk.

See the notes following the table.

Figure 7 (Page 2 of 2). 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**
7VMRAC20	191	3390	25+	36 000+	NOSFS	7VMRAC20 user ID's 191 minidisk. See note 6 on page 16 for additional storage requirements.
RACFVM	490	3390	70	100 800	NOSFS	Production CST/CMS system build disk.
RACFVM	305	3390	136	195 840	NOSFS	Production server code build disk.
RACFVM	200	3390	17	24 800	NOSFS	RACFVM primary database for non-SSI (3*)
RACFVM	200	3390	____	____	____	RACFVM primary database for SSI (4*)
RACFVM	300	3390	17	24 800	NOSFS	RACFVM backup database for non-SSI (3*)
RACFVM	300	3390	____	____	____	RACFVM backup database for SSI (4*)
RACFVM	301	3390	7	10 080	NOSFS	Primary SMF recording minidisk (7*)
RACFVM	302	3390	7	10 080	NOSFS	Secondary SMF recording minidisk (7*)
RACFVM	191	3390	9	12 960	NOSFS	RACFVM user ID's 191 minidisk
RACFSMF	191	3390	10+	14 400+	NOSFS	RACFSMF user ID's 191 minidisk See note 7 on page 16 for additional storage requirements.
RACFSMF	192	3390	10+	14 400+	NOSFS	RACFSMF user ID's 192 minidisk See note 7 on page 16 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	12 960	NOSFS	Backup RACFVM user ID's 191 minidisk.
IBMUSER	191	3390	1	1440	____	IBMUSER user ID's 191 minidisk
SYSADMIN	191	3390	1	1440	____	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 32 760 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 7VMRAC20's 191, 29E, 505, and 590 disks, and if possible they should be on separate control units.

3. The RACFVM 200 and 300 database disks should be on separate physical packs and separate control units.

4. For z/VM SSI installation, you must manually define the primary (virtual address 200) and backup (virtual address 300) RACF databases as two 3390 full-pack minidisks. It is required that the RACF database is shared between the members of an SSI cluster. See section 5.2.3, “Sharing a RACF Database” on page 11 for more information.

5. RACF supplies required virtual addresses for the RACF databases; **you must not change them**. The primary database is at virtual address 200; the backup database is 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.

6. On the 7VMRAC20 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.)

7. The size of the SMF recording minidisks should be governed by the amount of audit data recorded and the number of SECLABELS being audited.

8. 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.

9. Refer to section 5.2.4, “Restrictions When Using FBA Devices” on page 12 for FBA restrictions.

10. NOSFS means this disk cannot be a shared file system directory.

11. The 7VMRAC20 590 disk and the RACFVM 490 disk must be the same DASD type and size. Also these disks are defined as 70 cylinders and are RECOMPed to 63 cylinders.

5.4 ICHDEX01 Exit and Masked Passwords Considerations

Attention RACF users who are either migrating a pre-z/VM 5.4 RACF database to z/VM V7.2 OR migrating to z/VM V7.2 with a RACF database from a z/VM system on which the RACF ICHDEX01 exit is enabled. Without taking action, you may have users who will be unable to logon to the z/VM V7.2 system.

On z/VM 5.3 and earlier, the ICHDEX01 exit that was shipped by IBM was enabled by default. This exit (which returned return code 4) caused RACF to store passwords using a masking algorithm rather than DES encryption. Starting in z/VM 5.4, the ICHDEX01 exit was no longer enabled by default and passwords were no longer stored using the masking algorithm--but any passwords in masked format were able to be authenticated when a user having such a password logged on. Starting in z/VM 6.4, RACF no longer authenticates masked passwords, so any users who have passwords in masked format will no longer be able to log on the system. Instead users will receive an "invalid password" error message. This issue affects users who have older unexpired/non-expiring passwords.

Customers migrating a RACF database originating on a pre-z/VM 5.4 release, or customers migrating from a z/VM 6.3 or earlier release system on which the ICHDEX01 exit was enabled (which returned a return code 4), should take the following action before migrating to z/VM V7.2:

- Check for user profiles with password change dates older than the date when the current pre-z/VM V7.2 system was put into production.
- Check for user profiles which have non-expiring passwords.

Either of these situations might indicate masked passwords. In these cases, you should either change/reset the password OR enable an ICHDEX01 exit that returns return code 16, which allows RACF to authenticate masked passwords but store new passwords in DES encryption format (the default behavior between z/VM 5.4 and z/VM 6.3). The LISTUSER command can be used to determine when passwords were last updated. For information on masked passwords and the ICHDEX01 exit, refer to z/VM V7.2 RACF Security Server System Programmer's Guide, Chapter 3 "RACF Customization", in the section "Password Authentication Options".

Note: If the KDFAES algorithm is currently active on the pre z/VM V7.2 system (as determined by the SETROPTS LIST command), masking is not used, so NO action is needed.

6.0 Installation Instructions

Did you do an upgrade installation?

If you used the upgrade installation procedure documented in the *z/VM: Installation Guide* to upgrade a z/VM version 6 release 4 or version 7 release 1 system with RACF enabled to a z/VM version 7 release 2, no further enablement or customization is necessary. Your installation of RACF is complete. Proceed to Section 7.

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

RACF Security Server for z/VM is pre-installed on z/VM V7.2 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 enable 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 7 release 2 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. Upgrade the Database Templates" on page 23 through 6.15, "Task 13. Set Up the DirMaint-RACF Connector if DirMaint is Installed (Optional)" on page 41.

- 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 720.

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 20.

__ 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. Upgrade the Database Templates" on page 23.

__ 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 27.

__ Task 4. (*Optional*) Customize the RACFSMF user ID. Refer to 6.6, "Task 4. Customize the Processing of SMF Records (Optional)" on page 29.

__ Task 5. (*Optional*) Customize RACF within CP. Refer to 6.7, “Task 5. Customize RACF Within CP (Optional)” on page 30.

__ Task 6. Enable and Install the CP part of RACF for VM. Refer to 6.8, “Task 6. Install the CP Part of RACF” on page 31.

__ Task 7. (*Customers sharing RACF databases*) Change RACF database names. Refer to 6.9, “Task 7. Change RACF Database Names If Sharing with z/OS System” on page 32.

__ Task 8. IPL the CP system with RACF. Refer to 6.10, “Task 8. IPL the CP System with RACF” on page 33.

__ Task 9. Initialize or update the RACF database. Refer to 6.11, “Task 9. Update the RACF Database with Existing CP Directory Information” on page 34.

__ Task 10. (*Optional*) Create the global access table. Refer to 6.12, “Task 10. Create the Global Access Table (Optional)” on page 39.

__ Task 11. Set RACF options. Refer to 6.13, “Task 11. Set RACF Options” on page 39.

__ Task 12. (*Optional*) Determine audit and control options for VM events. Refer to 6.14, “Task 12. Determine Audit and Control Options for VM Events (Optional)” on page 40.

__ Task 13. (*Optional*) Set up dual registration. Refer to 6.15, “Task 13. Set Up the DirMaint-RACF Connector if DirMaint is Installed (Optional)” on page 41.

__ Task 14. Place RACF into production. Refer to 6.16, “Task 14. Place RACF Into Production” on page 42.

6.3 Task 1. Review Resources for Installing RACF

Procedural Note

Customers doing new non-SSI installations and not sharing existing RACF databases should review the information in 6.3.1, “General RACF User ID Information” on page 21 of this step and then skip to 6.5, “ Task 3. Prepare to Update RACF with Existing CP Directory Data” on page 27.

Customers sharing the RACF databases should review the information in 6.3.1, “General RACF User ID Information” on page 21 of this step and then continue with 6.3.2, “Sharing a RACF Database Information” on page 22.

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 *z/VM: RACF Security Server System Programmer's Guide*, section 'Recovery Procedures' for more information.

6.3.1 General RACF User ID Information

The planning information in the 7VMRAC20 PLANINFO file was used to create the 7VMRAC20, 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 RACF Security Server for z/VM user ID that owns the service resources (7VMRAC20), and the IBMUSER and SYSADMIN virtual machines are defined by single-configuration virtual machine definitions. All other RACF server virtual machines are defined by multiconfiguration virtual machine definitions. See *z/VM: CP Planning and Administration* for information on multiconfiguration and single-configuration virtual machine definitions.
- 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 7VMRAC20 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 IDENTITY 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.
- RACF supplies required virtual addresses for the RACF databases; you must not change these. The primary database is at virtual address 200; the backup database is at virtual address 300.
- 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 RACF database minidisks, RACFVM 200 and 300, have been formatted, allocated and initialized on the z/VM System deliverable using the RACF commands RACDSF, RACALLOC and RACINITD.

Procedural Note

Customers doing new non-SSI installations 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 27.

Customers using existing RACF databases and not sharing existing RACF databases should continue with step 6.4, “Task 2. Upgrade the Database Templates” on page 23.

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

6.3.2 Sharing a RACF Database Information

Attention

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

For z/VM single system image (SSI) environment, there are examples of RACF CP user directory entries in the section "Sharing RACF Databases in a z/VM Single System Image Cluster" in the *z/VM: RACF Security Server System Programmer's Guide*.

By default the CP user directory entries for the RACFVM and RACMAINT service machines do not configure the RACF database to be shared.

If you plan on sharing the RACF database between different real systems and/or multiple servers see *z/VM: RACF Security Server System Programmer's Guide* for more information on sharing a RACF database and *z/VM: CP Planning and Administration* for information on DASD Sharing.

Note: When RACF is installed in a single-member or multiple-member SSI environment, it is mandatory that the RACF database is shared. For information on sharing the RACF database in a z/VM single system image (SSI) see *z/VM: RACF Security Server System Programmer's Guide*.

Procedural Note

Customers using existing RACF databases should continue with step 6.4, “Task 2. Upgrade the Database Templates” on page 23 after setting up the RACF databases for sharing.

Customers doing new installations and not sharing the RACF databases should skip to step 6.5, “ Task 3. Prepare to Update RACF with Existing CP Directory Data” on page 27.

6.4 Task 2. Upgrade the Database Templates

Procedural Note

Customers using existing RACF databases should perform this step.

Customers doing new installations and not sharing the RACF database should skip to 6.5, “ Task 3. Prepare to Update RACF with Existing CP Directory Data” on page 27.

The RACF database must have templates at the function level 720 for RACF to function properly. If you are migrating from a previous release of RACF to RACF FL720, you must run the RACFCONV EXEC to upgrade the existing database templates to the current release.

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

Note: First run RACUT200 to verify the primary and backup databases. If either database has errors, they must be repaired before running RACFCONV. Reminder: It is highly recommended to keep a current copy of your primary RACF database distinct from your primary and backup volumes in case it is needed for recovery.

If you are sharing the RACF database, you must upgrade the templates from the system with the highest level of RACF.

Attention: Databases shared with z/OS

The RACF database templates supplied with RACF Security Server for z/VM FL720 are equivalent with those defined with the z/OS RACF V2.2. If you are sharing a RACF database with z/OS, z/OS RACF must be at:

- V2.2 or higher
- V2.1 plus the PTF's for APARs OA43998 and OA43999.

Attention:

If you are upgrading the first LPAR that is sharing a RACF database with other systems, or if you are upgrading the first member of an SSI cluster that is sharing a RACF database with other systems, you must force RACFVM off on all of the z/VM systems which are sharing that database in order to avoid database corruption.

For standalone systems issue FORCE RACFVM from the System Operator of that system.

To upgrade the database templates from a VM system use the following instructions. Note that database integrity should always be verified before an upgrade. For more information about RACF database integrity, see the White Paper: *Validating and Repairing RACF Database Integrity* at **www.**vm.ibm.com/security/. (To upgrade the database templates from a z/OS system, see *z/VM: RACF Security Server System Programmer's Guide*.)

1 You must force RACFVM off on all of the z/VM systems which are sharing that database in order to avoid database corruption.

For standalone systems:

- issue FORCE RACFVM from the OPERATOR user ID of each system.

For an SSI cluster, log on to OPERATOR and enter the following command for each member system:

- AT *system-name* CMD FORCE RACFVM

Disconnect from OPERATOR.

2 Logon to RACMAINT to verify the primary and backup RACF databases (200 and 300, respectively) before performing the RACF database template upgrade.

- **LINK RACFVM 490 490 RR**
- **IPL 490**

- **LINK RACFVM 305 305 RR**
- **ACCESS 305 B**
- **LINK RACFVM 200 200 RR**
- **LINK RACFVM 300 300 RR**
- **ACCESS 190 T**

Then run the RACUT200 utility:

- Enter **RACUT200**
- Reply **YES** to the 'Do you want to Verify a RACF database?' prompt.
- If a RACVERFY FILE input file exists, you will be given the option to reuse it or overlay it. If a RACVERFY FILE does not exist, one will be created and XEDIT will be entered. Type **FILE** when editing is complete.
- Reply **200** to the 'Enter the Input device address' prompt.
- Press **Enter** to bypass copy.
- Reply **Yes** to the 'Do you wish to continue?' prompt.
- Message RPIOPN003E and IRR62003I can be ignored. You may also get messages DMSLOS013E and IRR62064I.
- Return code from 'IRRUT200'= 0 should be issued if successful. Return code 0 implies that your RACF database 200 has no errors.
- The IRRUT200 output report will be sent to your virtual printer. If you received a non-0 return code from **RACUT200**, you should analyze the output that was placed in your virtual printer. Peek or xedit the output file, and do a quick locate for errors: search for "IRR62" messages and "LOCATIONS WITH POSSIBLE CONFLICTS". You may find errors in RACF PROFILEs, or RBA errors in the RACF database. These errors will need to be corrected before running the RACFCONV utility.

Also, rerun the RACUT200 utility for the RACF backup database 300 and verify it completes with return code 0.

If RACUT200 output for 200 or 300 RACF databases shows errors:

- you may need to contact IBM Support to help you repair the RACF databases
- use 'last good copies' of these RACF databases
- see the Chapter "Recovery Procedures" in the z/VM RACF Security Server System Programmer's Guide.

  In many cases, running RACUT400 to perform a copy of the RACF database, will repair most and possibly all of the errors.

Once RACUT200 completes with return code 0, you can continue to the next step to run RACFCONV.

3 Logon to RACMAINT then run RACFCONV EXEC to upgrade 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, template update was applied.
Ready; T=0.07/0.10 11:41:46
```

Note: For non zero return codes see z/VM: RACF Security Server System Programmer's Guide.

```
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, template update was applied.
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

Only customers performing a new installation should perform this task.

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 7VMRAC20 user ID.

2 Ensure that you have access to your CP directory file. (The default CP directory file name is USER DIRECT and it resides on PMAINT's 2CC minidisk.)

3 If you are currently running DirMaint then you need to issue the DIRM USER WITHPASS command and put the resulting file on 7VMRAC20'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.

4 Ensure that the 7VMRAC20 191 disk has enough free space and that the user ID building the database (later in the installation) has access to the 7VMRAC20 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 651 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 use either the QUIET option of RPIDIRCT to suppress the console output, or the DISK option to write the console output to the file RPIDIRCT OUTLIST. Type `RPIDIRCT ?` for details on how to specify the QUIET or DISK option.

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

Servicing RACF uses the z/VM automated service commands therefore you **MUST** give UACC of UPDATE for VMRDR to the MAINT720 user ID in the RPIDIRCT SYSUT1 file.

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

Procedural Note

This step is optional, but highly recommended. If archiving of SMF records is not performed, valuable security audit information may be lost.

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*.

6.7 Task 5. Customize RACF Within CP (Optional)

> **Procedural Note**
>
> This step is optional.
>
> The method used to apply a local modification to RACF is shown in the chapter "Applying local service and local modifications" of the *z/VM: Service Guide*. If you choose to customize RACF within CP as part of the installation process you do not need to perform the SERVICE *compname* BUILD and PUT2PROD steps of the local modification procedure as these steps will be performed later as part of the RACF/VM installation.

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

For information on how to customize the RACF options, see *z/VM: RACF Security Server System Programmer's Guide*

6.8 Task 6. Install the CP Part of RACF

Procedural Note

All customers should perform this step.

If you are enabling the RACF security server for z/VM in an SSI cluster, you only need to perform this step from one member of that cluster where this new release of RACF is to be enabled.

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, HCPRPP, 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 In order to use RACF once you have acquired a license for it, you need to follow the instructions in the ***MEMO TO USERS for IBM RACF Security Server for z/VM, function level 720*** to enable it for use.

After the steps in the MEMO have been completed the new CP nucleus, with the RACF CP parts, will be 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.

6.9 Task 7. 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 6.10, “Task 8. IPL the CP System with RACF” on page 33.

If the RACF database names on the z/OS system are different than those defaulted for VM (RACF.DATASET and RACF.BACKUP), you need to change the RACF database names in the ICHRDSNT ASSEMBLE and ICHRDSNT TEXT files to match the z/OS system.

To change the ICHRDSNT ASSEMBLE and TEXT files you must perform a local modification against them. Follow the steps documented in chapter "RACF Customization", section "The Database Name Table" of the *z/VM: RACF Security Server System Programmer's Guide*

6.10 Task 8. IPL the CP System with RACF

Procedural Note

All customers should perform this step.

If this step is being performed in an SSI cluster, you only need to perform it from one member of that cluster where this new release of RACF is to be enabled.

Note: An SSI cluster cannot contain a mixture of RACF enabled and non-RACF enabled members.

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 MAINT720 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 6.8, “Task 6. Install the CP Part of RACF” on page 31.

To IPL from the CF2 parm disk follow the instructions in *z/VM: Service Guide*, appendix B, in the section titled "IPLing with a test level of the CPLOAD MODULE".

3 IPL with **NOAUTOLOG**.

When you see the following messages 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.

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

XAUTOLOG RACMAINT

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

6.11 Task 9. Update the RACF Database with Existing CP Directory Information

Procedural Note

Only customers performing a new installation should perform this task.

If this step is being performed in an SSI cluster, you only need to perform it from one member of that cluster where this new release of RACF is to be enabled.

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 27.

Procedural Note

If you are **not sharing** existing RACF databases with another system, continue with section 6.11.1, “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 6.11.2, “Update the RACF Database (If You Are Sharing an Existing Database)” on page 38.

6.11.1 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.

6.11.1.1 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 correct any incorrect entries in HCPRWA and regenerate the CP nucleus. See *z/VM: RACF Security Server System Programmer's Guide* for more information on RACF Customization and setting the CP disposition for access requests.

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

6.11.1.2 Building the RACF Database

1 Link and access 7VMRAC20's 505, 191, and 29E disks

```
link 7VMRAC20 505 305 rr
acc 305 c
link 7VMRAC20 191 192 rr
acc 192 b
link 7VMRAC20 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.

6.11.1.3 Defining the Security Administrator and Maintenance User IDs.

In 6.3, “Task 1. Review Resources for Installing RACF” on page 20 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.

Note: Because SYSADMIN is an IBM-defined user ID, it might be the target for unauthorized access to your system. To prevent this, it is recommended that you define a security administrator user ID named according to your installation standards.

2 Give the z/VM system maintenance user IDs RACF OPERATIONS authority (in order to use the VMSES/E SERVICE and PUT2PROD commands to install service).

Note: You only need the altuser for MIGMAINT when you perform a z/VM upgrade installation.

```
RAC ALTUSER MAINT720 OPERATIONS
RAC ALTUSER BLDSEG OPERATIONS
RAC ALTUSER BLDRACF OPERATIONS
RAC ALTUSER BLDNUC OPERATIONS
RAC ALTUSER BLDCMS OPERATIONS
RAC ALTUSER MIGMAINT OPERATIONS
```

MAINT720 is the default maintenance user ID that is used by the automated VMSES/E service commands.

BLD*xxx* is autologged by MAINT720 as required when service is being installed.

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 7VMRAC20 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 6.12, “Task 10. Create the Global Access Table (Optional)” on page 39.

6.11.2 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 7VMRAC20's 505, 191, and 29E disks.

```
detach 505
detach 305
link 7VMRAC20 505 305 rr
acc 305 c
link 7VMRAC20 191 192 rr
acc 192 b
link 7VMRAC20 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.

6.12 Task 10. Create the Global Access Table (Optional)

Procedural Note

This step is optional.

If this step is being performed in an SSI cluster, you only need to perform it from one member of that cluster where this new release of RACF is to be enabled.

If you choose not to perform this step, skip to 6.13, “Task 11. Set RACF Options.”

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.

6.13 Task 11. Set RACF Options

Procedural Note

If this step is being performed in an SSI cluster, you only need to perform it from one member of that cluster where this new release of RACF is to be enabled.

In order to use the VMSES/E SERVICE and PUT2PROD service commands when RACF is enabled you have to provide access authorization for the following general resource classes as required by your installation:

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

Important Installation Note:

SURROGAT class must be activated for z/VM 720 RACF install. Many of the install and system userids are LOGON BY only. The default LOGON BY userid is IBMVM1. More information on IBMVM1 can be found in Chapter 7 of the *z/VM: Installation Guide*

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 as required by your installation.

For information on activating general resource classes see *z/VM RACF Security Server Security Administrator's Guide*.

6.14 Task 12. Determine Audit and Control Options for VM Events (Optional)

Procedural Note

This step is optional.

If this step is being performed in an SSI cluster, you only need to perform it from one member of that cluster where this new release of RACF is to be enabled.

If you choose not to perform this step, skip to 6.15, “Task 13. Set Up the DirMaint-RACF Connector if DirMaint is Installed (Optional)” on page 41.

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

- APPCPWVL
- COUPLE.G
- DIAG0A0
- DIAG0D4
- DIAG0E4
- DIAG088
- DIAG280

- FOR.C
- FOR.G
- LINK
- MDISK
- RSTDSEG
- STORE.C
- TAG
- TRANSFER.D
- TRANSFER.G
- TRSOURCE
- RDEVCTRL

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*.

6.15 Task 13. Set Up the DirMaint-RACF Connector if DirMaint is Installed (Optional)

Procedural Note

This step is optional.

If you choose not to perform this step, skip to 6.16, “Task 14. Place RACF Into Production” on page 42.

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 7VMDIR20 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. You must give the DIRMAINT user ID RACF administrator SPECIAL authority.
3. 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.

Note: This step should be performed after RACF is put into production. The ESM_LOG_RECORDING_EXIT issues RACROUTE requests which are sent to the RACF service machine that is identified in the RACF SERVMACH file that resides on the CMS (19E) y-disk. The default is set to RACFVM.

4. 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'.

6.16 Task 14. Place RACF Into Production

Procedural Note

All customers should perform this step.

If you are enabling the RACF Security Server for z/VM in an SSI cluster, you must perform this step on every member of the SSI where this new release of RACF is to be copied into production.

6.16.1 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 MAINT720 to put RACF code on to the production build disks.

2 You must start the shared filepool server machines.

```
xautolog autolog1
```

3 This step will:

- Copy any outstanding service from an RSU application applied before the enablement of RACF to the appropriate production build disk.
- Copy any local modifications made during RACF installation to the appropriate production build disk.
- Place CPLOAD MODULE with RACF in it on the CF1 parm disk.

```
put2prod racf
put2prod cp
```

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

```
link 7VMRAC20 599 599 rr
access 599 e
access ispf-fm f
vmfcopy * * e = = f (prodid 7VMRAC20%RACF olddate replace
```

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

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 MAINT720.

b Copy the ISPF general user code.

```
link 7VMRAC20 599 599 rr
access 599 e
access 19e f
vmfcopy RACF EXEC e = = f2 (prodid 7VMRAC20%RACF olddate replace
vmfcopy ICHSPF00 LOADLIB e = = f2 (prodid 7VMRAC20%RACF olddate replace
vmfcopy DUALREG PROFILE  e = = f2 (prodid 7VMRAC20%RACF olddate replace
vmfcopy DUALREG SKELETON e = = f2 (prodid 7VMRAC20%RACF olddate replace
```

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

6 Set up the AUTOLOG1 and AUTOLOG2 user IDs.

Procedural Note

Customers doing new installations 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 7VMRAC20
force MAINT720
force RACMAINT
xautolog RACFVM

8 At this time your system is still IPL'ed using the CPLOAD Module from the secondary parm disk (CF2). The next time you IPL, you will IPL using 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

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

7.1 Servicing RACF

Use the service instructions documented in the *z/VM: Service Guide* to install (receive, apply, build and place into production) preventive and corrective service to RACF.

Appendix A. Set up the RACF ISPF Panels

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 A.1, “Modify the ISPF Files For Use With PDF.”
- If you have ISPF installed, continue with section A.2, “Modify the ISPF Files for use with non-PDF” on page 49.

A.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.

A.1.1 Step 1 - Modify the ISPF EXEC Filedefs

Figure 8 on page 47 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 7VMRAC20 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 8. 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

A.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')'
```

A.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 A.6, “Full Part Replacement (Not Assemble) - Example” on page 54 to perform the local modification to the ICHP00 COPY file. Use the following substitution values:

- For *fn* use **ICHP00**
- For *ft* use **ISPF**
- 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 7VMRAC20's 599 test build disk.

Where to next?

Continue with A.3, “Modify the ISPF Primary Option Panel” on page 53.

A.2 Modify the ISPF Files for use with non-PDF

A.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 9.

```
/*                                                               */
/* 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 9. 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

A.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.

A.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.

A.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 A.6, “Full Part Replacement (Not Assemble) - Example” on page 54 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 7VMRAC20's 599 test build disk.

A.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 10 on page 52.

Follow the steps documented in A.6, “Full Part Replacement (Not Assemble) - Example” on page 54 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 7VMRAC20'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 10. Changes for RACF EXEC INIT Routine for Systems without PDF

A.3 Modify the ISPF Primary Option Panel

A sample ISPF Primary Option Panel (ISRPRIM SAMPLE) is supplied on the 7VMRAC20 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.

A.4 Dual Registration Users Only

Procedural Note

If you are not using dual registration skip to A.5, “Invoke the RACF ISPF Panels” on page 54.

A.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 A.6, “Full Part Replacement (Not Assemble) - Example” on page 54 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 7VMRAC20's 599 test build disk.

A.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 A.6, "Full Part Replacement (Not Assemble) - Example" 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 7VMRAC20's 599 test build disk.

A.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.

A.6 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 7VMRAC20's minidisk access order.

```
access 590 t
vmfsetup 7VMRAC20 {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-abbrvLnnnn 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 7VMRAC20 vvtlcl e tdata :mod lclnnnn :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 7VMRAC20 {RACF | RACFSFS } blist memname (all
```

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

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:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, 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
Bldg 707-1
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. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Privacy Policy Consideration

IBM Software products, including software as a service solutions, ("Software Offerings) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If the Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see the IBM Online Privacy Policy at http://www.ibm.com/privacy and the IBM Online Privacy Statement at http://www.ibm.com/privacy/details, in particular the section entitled "Cookies, Web Beacons and Other Technologies , and the IBM Software Products and Software-as-a-Service Privacy Statement at http://www.ibm.com/software/info/product-privacy.

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 IBM copyright and trademark information - United States:

www.ibm.com/legal/us/en/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.

Index

A

assembler requirements 11
AUTOLOG1 user ID 44
AUTOLOG2 user ID 44

B

books
  RACF 4
  VM 5

C

COMPID value for RETAIN 7
CP directory on VM
  migrating data to the RACF database from 27

D

DASD
  FBA 11, 12
  requirements for RACF 13
  shared 11
database name table (ICHRDSNT) 33
database templates, updating 23
database, RACF
  changing the names of 32
  initializing 35
  migrating data to from the CP directory 27
  RACFCONV EXEC 23
  sharing 11
  sharing with z/OS system 32
  updating 38
  updating the templates 23
devices, FBA 11, 12
DirMaint
  recording activity in RACF SMF records 41
  requirements for dual registration 11
  setting up DirMaint-RACF Connector 41
dual registration 53
  requirements for 11

E

events, VM 40
EXECs
  ICHSFSIN 50
  RACFCONV 23

F

FBA DASD 11, 12
FESN value for RETAIN 7

G

global access table 39

H

hardware requirements 10
HASM, use of 11
HLASM, requirement for 11

I

IBMUSER user ID 35
ICHRDSNT
  changing 32
  errors in during initialization 33
ICHSFSIN EXEC 50
IPL VM system 33
ISPF
  installing the RACF panels 46
  invoking the RACF panels 54
  modifying the EXECs for 46
  requirements 10
  requirements for dual registration 11

L

level required 10

M

minidisk
  requirements for RACF 13

O

operating system requirements 10
operator prompts
  during IPL 33

P

panels, RACF
  installing 46
  invoking 54
program number for RACF 3
program product requirements 10
prompts to operator during IPL
PSP UPGRADE and SUBSET values 6
publications
  RACF 4
  VM 5

R

RACF
  description 1
  IBM support for 6
  program number 3
RACFCONV EXEC 23
RACFSMF user ID
  function of 29
RACFVM
  logging on 44
release value for RETAIN 7
requirements
  assembler 11
  hardware 10
  ISPF 10
  operating system 10
  program products 10
RETAIN COMPID, release, and FESN values 7
RPIBLDDS 36
RPIDIRCT EXEC 27
RPIDIRCT SYSUT1
  how used 27
  initializing the RACF database with 35
  running the commands in 36
  updating the RACF database with 38

S

SETEVENT command 41
sharing a RACF database 11
SMF CONTROL file
  function of 30
SMF DATA file 29
SMF records
  controlling processing of 29
  recording DirMaint activity in 41
software requirements 10
storage requirements for RACF 13

T

templates, updating 23

U

user IDs
  AUTOLOG1 44
  AUTOLOG2 44
  IBMUSER 35
  RACFVM 44
  required for RACF 13

V

VM events, auditing and controlling 40
VM, level required 10
VMSES/E 13
VMXEVENT profile 41

Reader's Comments

IBM® RACF Security Server for z/VM, function level 720

You may use the VM Feedback page (Reader's Comments) on the z/VM Web site at:

www.vm.ibm.com/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.

Program Number: 5741-A09

Printed in USA

GI13-4364-01