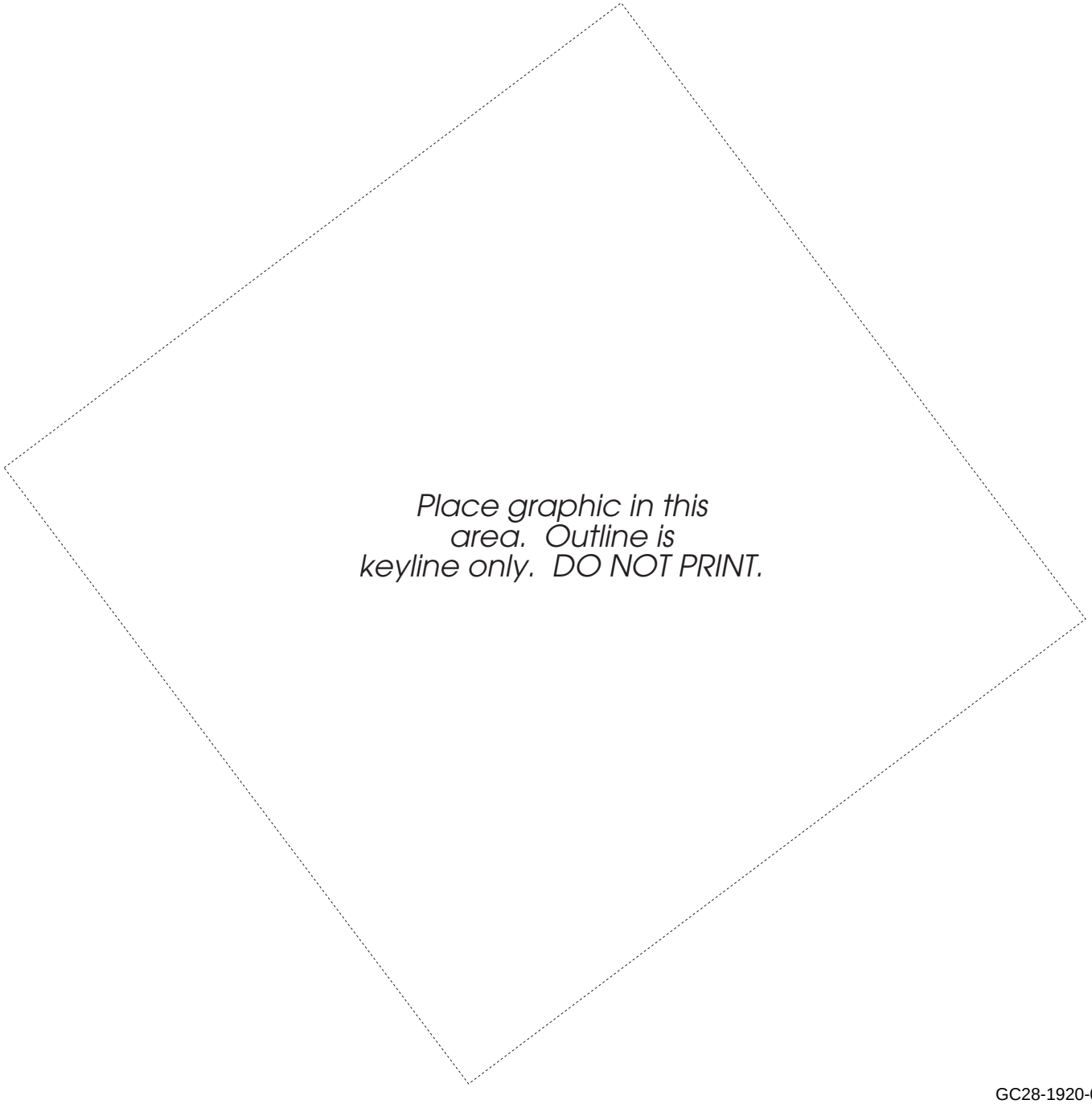
OS/390

Security Server (RACF) Planning: Installation and Migration



GC28-1920-01

OS/390

Security Server (RACF) Planning: Installation and Migration

GC28-1920-01

Note

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

Second Edition, September 1996

This is a major revision of GC28-1920-00.

This edition applies to Version 1 Release 2 of OS/390 (5645-001) and to all subsequent releases and modifications until otherwise indicated in new editions.

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

IBM welcomes your comments. A form for readers' comments may be provided at the back of this publication, or you may address your comments to the following address:

International Business Machines Corporation
Department 55JA, Mail Station P384
522 South Road
Poughkeepsie, NY 12601-5400
United States of America

FAX (United States & Canada): 1+914+432-9405
FAX (Other Countries):
Your International Access Code +1+914+432-9405

IBMLink (United States customers only): KGNVMC(MHVRCFS)
IBM Mail Exchange: USIB6TC9 at IBMMAIL
Internet e-mail: mhvrcfs@vnet.ibm.com
World Wide Web: http://www.s390.ibm.com/os390

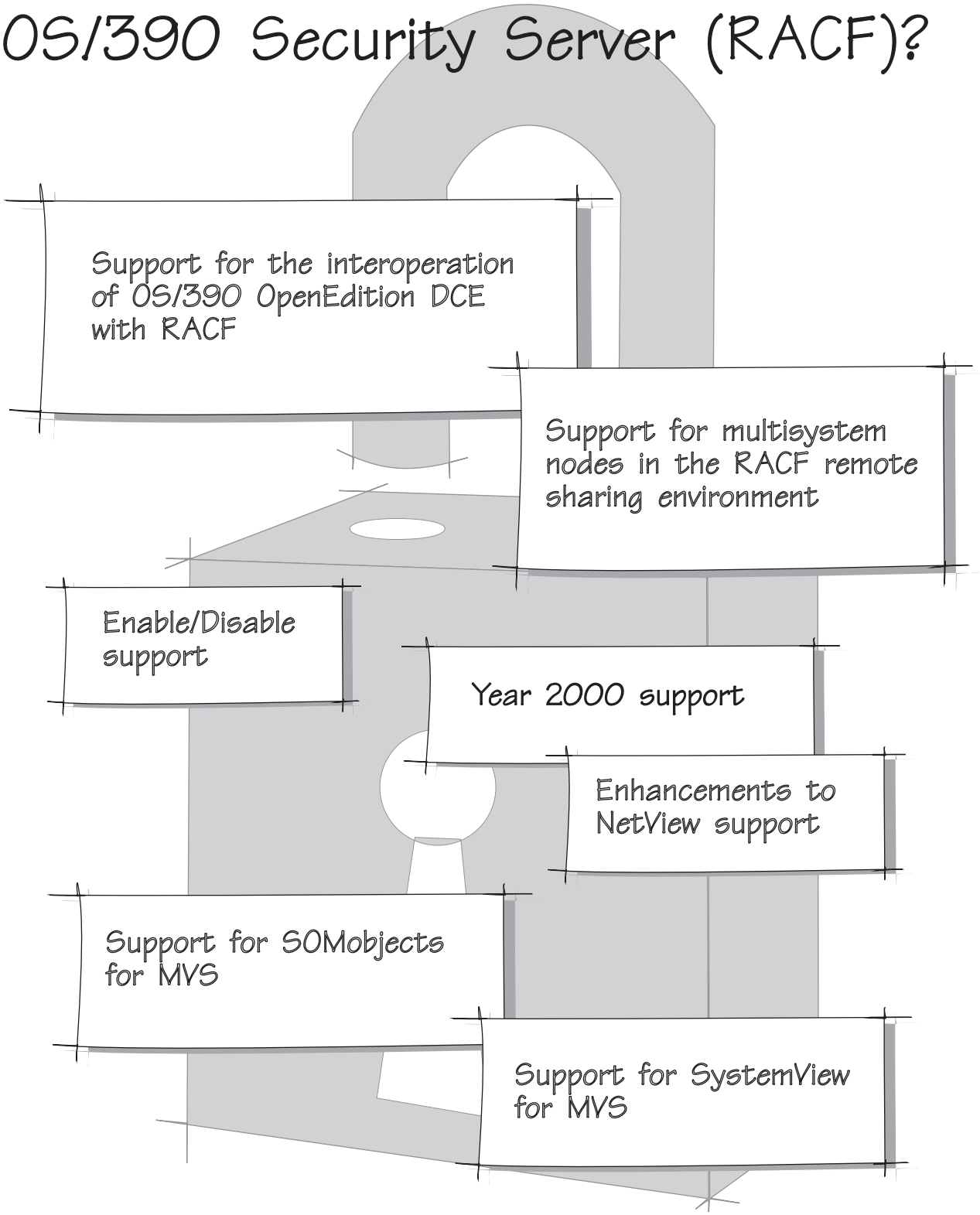
If you would like a reply, be sure to include your name, address, telephone number, or FAX number.

Make sure to include the following in your comment or note:

- Title and order number of this book
- Page number or topic related to your comment

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.

What's New in Release 2 for OS/390 Security Server (RACF)?



Contents

Figures

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates.

Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program or service may be used. A functionally equivalent product, program, or service which does not infringe on any of IBM's intellectual property rights may be used instead of the IBM product, program or service. Evaluation and verification of operation in conjunction with other products, programs, or services, except those expressly designated by IBM, is the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
USA

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

IBM Corporation
Mail Station P300
522 South Road
Poughkeepsie, NY 12601-5400
USA
Attention: Information Request

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

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

- AS/400
- BookManager
- CICS
- CICS/ESA
- DB2
- DFSMS
- DFSMS/MVS
- IBM
- IBMLink
- IMS
- Library Reader
- MVS
- MVS/ESA
- MVS/XA
- NetView
- OpenEdition
- OS/2
- OS/390
- Parallel Sysplex
- RACF
- RETAIN
- SOM
- SOMobjects
- SystemView
- S/390
- System/390
- TalkLink
- VM/ESA
- VM/XA

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Windows is a trademark of Microsoft Corporation.

Other company, product, and service names, which may be denoted by a double asterisk (**), may be trademarks or service marks of others.

About This Book

This book contains information about the Resource Access Control Facility (RACF), which is part of the OS/390 Security Server. The Security Server has two components:

- RACF
- OpenEdition DCE Security Server

For information about the OpenEdition DCE Security Server, see the publications related to that component.

This book provides information to guide you through the migration process from OS/390 Release 1 Security Server (RACF) or RACF 2.2 to OS/390 Release 2 Security Server (RACF).

The purpose of this book is to ensure an orderly transition to a new RACF release. It is *not* intended for customers installing RACF for the first time or installing a release prior to Security Server (RACF) Release 2. First-time RACF customers should read *OS/390 Security Server (RACF) Introduction* and use the program directory shipped with the product when they are ready to install the product.

Who Should Use This Book

This book is intended for experienced system programmers responsible for migrating from OS/390 Release 1 Security Server (RACF) or RACF 2.2 to OS/390 Release 2 Security Server (RACF). This book assumes you have knowledge of OS/390 Release 1 Security Server (RACF) or RACF 2.2.

If you are migrating from a RACF release prior to 2.2, you should also read previous versions of this book, as described in “Migration Paths for OS/390 Release 2 Security Server (RACF)” on page 23.

How to Use This Book

This book is organized in the following order:

- Chapter 1, “Planning for Migration” on page 1, provides information to help you plan your installation's migration to the new release of RACF.
- Chapter 2, “Release Overview” on page 5, provides an overview of support in the new release.
- Chapter 3, “Summary of Changes to RACF Components for OS/390 Release 2” on page 13, lists specific new and changed support for the new release.
- Chapter 4, “Planning Considerations” on page 23, describes high-level migration considerations for customers upgrading to the new release of RACF from previous levels of RACF.
- Chapter 5, “Installation Considerations” on page 27, highlights information about installing the new release of RACF.
- Chapter 6, “Customization Considerations” on page 35, highlights information about customizing function to take advantage of new support after the new release of RACF is installed.

- Chapter 7, “Administration Considerations” on page 37, summarizes changes to administration procedures for the new release of RACF.
- Chapter 8, “Auditing Considerations” on page 45, summarizes changes to auditing procedures for the new release of RACF.
- Chapter 9, “Operational Considerations” on page 49, summarizes changes to operating procedures for the new release of RACF.
- Chapter 10, “Application Development Considerations” on page 51, identifies changes in the new release of RACF that might require changes to an installation's existing programs.
- Chapter 11, “General User Considerations” on page 55, summarizes new support that may affect general user procedures.
- Chapter 13, “Scenarios” on page 61, contains migration scenarios illustrating steps customers might take in migrating to the new release of RACF in different situations.

Where to Find More Information

Where necessary, this book references information in other books. For complete titles and order numbers for all products that are part of OS/390, see *OS/390 Information Roadmap*, GC28-1727.

Softcopy Publications

The OS/390 Security Server (RACF) library is available on the following CD-ROMs. The CD-ROM collections include the IBM Library Reader, a program that enables customers to read the softcopy books.

- The *OS/390 Security Server (RACF) Information Package*, SK2T-2180

  This softcopy collection kit contains the OS/390 Security Server (RACF) library. It also contains the RACF/MVS Version 2 product libraries, the RACF/VM 1.10 product library, product books from the OS/390 and VM collections, International Technical Support Organization (ITSO) books, and Washington System Center (WSC) books that contain substantial amounts of information related to RACF. The kit does not contain any licensed publications. By using this CD-ROM, you have access to RACF-related information from IBM products such as OS/390, VM, CICS, and NetView without maintaining shelves of hardcopy documentation or handling multiple CD-ROMs. To get more information on the *OS/390 Security Server (RACF) Information Package*, see the advertisement at the back of the book.

- The *OS/390 Collection Kit*, SK2T-6700

  This softcopy collection contains a set of OS/390 and related product books. This kit contains both unlicensed and licensed books.

- The *Online Library Omnibus Edition MVS Collection Kit,* SK2T-0710

  This softcopy collection contains a set of key MVS and MVS-related product books. It also includes the RACF Version 2 product libraries. *OS/390 Security Server (RACF) Messages and Codes* is also available as part of *Online Library Productivity Edition Messages and Codes Collection,* SK2T-2068.

RACF Courses

The following RACF classroom courses are also available:

- *Effective RACF Administration,* H3927
- *MVS/ESA RACF Security Topics,* H3918
- *Implementing RACF Security for CICS/ESA,* H3992

IBM provides a variety of educational offerings for RACF. For more information on classroom courses and other offerings, see your IBM representative, *IBM Mainframe Training Solutions*, GR28-5467, or call 1-800-IBM-TEACH (1-800-426-8322).

IBM Systems Center Publications

IBM systems centers produce “red” and “orange” books that can be helpful in setting up and using RACF.

These books have not been subjected to any formal review nor have they been checked for technical accuracy, but they represent current product understanding (at the time of their publication) and provide valuable information on a wide range of RACF topics. They are not shipped with RACF. You must order them separately. A selected list of these books follows:

- *Systems Security Publications Bibliography,* G320-9279
- *Elements of Security: RACF Overview - Student Notes,* GG24-3970
- *Elements of Security: RACF Installation - Student Notes,* GG24-3971
- *Elements of Security: RACF Advanced Topics - Student Notes,* GG24-3972
- *RACF Version 2 Release 2 Technical Presentation Guide,* GG24-2539
- *RACF Version 2 Release 2 Installation and Implementation Guide*, SG24-4580
- *Enhanced Auditing Using the RACF SMF Data Unload Utility,* GG24-4453
- *RACF Macros and Exit Coding,* GG24-3984
- *RACF Support for Open Systems Technical Presentation Guide,* GG26-2005
- *DFSMS and RACF Usage Considerations,* GG24-3378
- *Introduction to System and Network Security: Considerations, Options, and Techniques,* GG24-3451
- *Network Security Involving the NetView Family of Products,* GG24-3524
- *System/390 MVS Sysplex Hardware and Software Migration,* GC28-1210
- *Secured Single Signon in a Client/Server Environment,* GG24-4282
- *Tutorial: Options for Tuning RACF,* GG22-9396

Other books are available, but they are not included in this list either because the information they present has been incorporated into IBM product manuals or because their technical content is outdated.

Other Sources of Information

IBM provides customer-accessible discussion areas where RACF may be discussed by customer and IBM participants. Other information is available through the Internet.

IBM Discussion Areas

Two discussion areas provided by IBM are the MVSRACF discussion and the SECURITY discussion.

- **MVSRACF**

  MVSRACF is available to customers through IBM's TalkLink offering. To access MVSRACF from TalkLink:

  1. Select S390 (the S/390 Developers' Association)
  2. Use the fastpath keyword: MVSRACF

- **SECURITY**

  SECURITY is available to customers through IBM's DialIBM offering, which may be known by other names in various countries. To access SECURITY:

  1. Use the CONFER fastpath option
  2. Select the SECURITY CFORUM

Contact your IBM representative for information on TalkLink, DialIBM, or equivalent offerings for your country, and for more information on the availability of the MVSRACF and SECURITY discussions.

Internet Sources

The following resources are available through the Internet:

- **RACF home page**

  You can visit the RACF home page on the World Wide Web using this address:

  http://www.s390.ibm.com/products/racf/racfhp.html

- **RACF-L discussion list**

  Customers and IBM participants may also discuss RACF on the RACF-L discussion list. RACF-L is not operated or sponsored by IBM; it is run by the University of Georgia.

  To subscribe to the RACF-L discussion, so you can receive postings, send a note to:

  listserv@uga.cc.uga.edu

  Include the following line in the body of the note, substituting your first name and last name as indicated:

  subscribe racf-l *first_name last_name*

  To post a question or response to RACF-L, send a note to:

  racf-l@uga.cc.uga.edu

  Include an appropriate `Subject:` line.

- **Sample code**

You can get sample code, internally-developed tools, and exits to help you use RACF. All this code works[1], but is not officially supported. Each tool or sample has a README file that describes the tool or sample and any restrictions on its use.

The simplest way to reach this code is through the RACF home page. From the home page, click on **System/390 FTP Servers** under the topic, "RACF Sample Materials."

The code is also available from **lscftp.pok.ibm.com** through **anonymous ftp**.

To get access:

1. Log in as user **anonymous**
2. Change the directory (**cd**) to **/pub/racf/mvs** to find the subdirectories that contain the sample code. We'll post an announcement on RACF-L, MVSRACF, and SECURITY CFORUM whenever we add anything.

Restrictions

Because the sample code and tools are not officially supported,

- There are no guaranteed enhancements
- No APARs can be accepted

The name and availability of the **ftp** server may change in the future. We'll post an announcement on RACF-L, MVSRACF, and SECURITY CFORUM if this happens.

However, even with these restrictions, it should be useful for you to have access to this code.

To Request Copies of IBM Publications

Direct your request for copies of any IBM publication to your IBM representative or to the IBM branch office serving your locality.

There is also a toll-free customer support number (1-800-879-2755) available Monday through Friday from 6:30 a.m. through 5:00 p.m. Mountain time. You can use this number to:

- Order or inquire about IBM publications
- Resolve any Software Manufacturing or delivery concerns
- Activate the Program Reorder Form to provide faster and more convenient ordering of software updates

See the advertisement at the back of the book for information about the *OS/390 Security Server (RACF) Information Package*.

[1] In our environment, at the time we make it available

Elements and Features in OS/390

You can use the following table to see the relationship of a product you are familiar with and how it is referred to in OS/390 Release 2. OS/390 Release 2 is made up of elements and features that contain function at or beyond the release level of the products listed in the following table. The table gives the name and level of each product on which an OS/390 element or feature is based, identifies the OS/390 name of the element or feature, and indicates whether it is part of the base or optional. For more compatibility information about OS/390 elements see *OS/390 Up and Running!*, GC28-1726.

Product Name and Level	Name in OS/390	Base or Optional
BookManager BUILD/MVS V1R3	BookManager BUILD	optional
BookManager READ/MVS V1R3	BookManager READ	base
MVS/Bulk Data Transfer V2	Bulk Data Transfer (BDT)	base
MVS/Bulk Data Transfer File-to-File V2	Bulk Data Transfer (BDT) File-to-File	optional
MVS/Bulk Data Transfer SNA NJE V2	Bulk Data Transfer (BDT) SNA NJE	optional
IBM OS/390 C/C++ V1R2	C/C++	optional
DFSMSdfp V1R3	DFSMSdfp	base
DFSMSdss	DFSMSdss	optional
DFSMShsm	DFSMShsm	optional
DFSMSrmm	DFSMSrmm	optional
DFSMS/MVS Network File System V1R3	DFSMS/MVS Network File System	base
DFSORT R13	DFSORT	optional
EREP MVS V3R5	EREP	base
FFST/MVS V1R2	FFST/MVS	base
GDDM/MVS V3R2 • GDDM-OS/2 LINK • GDDM-PCLK	GDDM	base
GDDM-PGF V2R1.3	GDDM-PGF	optional
GDDM-REXX/MVS V3R2	GDDM-REXX	optional
IBM High Level Assembler for MVS & VM & VSE V1R2	High Level Assembler	base
IBM High Level Assembler Toolkit	High Level Assembler Toolkit	optional
ICKDSF R16	ICKDSF	base
ISPF V4R2	ISPF	base
Language Environment for MVS & VM V1R5	Language Environment	base
Language Environment V1R5 Data Decryption	Language Environment Data Decryption	optional
MVS/ESA SP V5R2.2 • BCP • ESCON Director Support • Hardware Configuration Definition (HCD) • JES2 V5R2.0 • JES3 V5R2.1 • LANRES/MVS V1R3.1 • IBM LAN Server for MVS V1R1 • MICR/OCR Support • OpenEdition System Services	 • BCP or MVS • ESCON Director Support • Hardware Configuration Definition (HCD) • JES2 • JES3 • LANRES • LAN Server • MICR/OCR Support • OpenEdition System Services	 base base base base optional base base base base

Product Name and Level	Name in OS/390	Base or Optional
• OpenEdition Application Services • OpenEdition DCE Base Services (OSF DCE level 1.1) • OpenEdition DCE Distributed File Service (DFS) (OSF DCE level 1.1) • OpenEdition DCE User Data Privacy • SOMobjects Application Development Environment (ADE) V1R1 • SOMobjects Runtime Library (RTL) • SOMobjects service classes	• OpenEdition Application Services • OpenEdition DCE Base Services • OpenEdition DCE Distributed File Service (DFS) • OpenEdition DCE User Data Privacy • SOMobjects Application Development Environment (ADE) • SOMobjects Runtime Library (RTL) • SOMobjects service classes	base base base optional optional base base
Open Systems Adapter Support Facility (OSA/SF) R1	Open Systems Adapter Support Facility (OSA/SF)	base
MVS/ESA RMF V5R2	RMF	optional
RACF V2R2	Security Server • RACF • OpenEdition DCE Security Server	optional
SDSF V1R6	SDSF	optional
SMP/E	SMP/E	base
	Softcopy Print	base
SystemView for MVS Base	SystemView for MVS Base	base
IBM TCP/IP V3R1 • TCP/IP CICS Sockets • TCP/IP IMS Sockets • TCP/IP Kerberos • TCP/IP Network Print Facility (NPF) • TCP/IP OpenEdition Applications • TCP/IP OS/2 Offload	TCP/IP • TCP/IP CICS Sockets • TCP/IP IMS Sockets • TCP/IP Kerberos • TCP/IP Network Print Facility (NPF) • TCP/IP OpenEdition Applications • TCP/IP OS/2 Offload	base optional optional optional optional optional optional
TIOC R1	TIOC	base
Time Sharing Option Extensions (TSO/E) V2R5	TSO/E	base
VisualLift for MVS V1R1.1	• VisualLift Run-Time Environment (RTE) • VisualLift Application Development Environment (ADE)	base optional
VTAM V4R3 with the AnyNet feature	VTAM	base
3270 PC File Transfer Program V1R1.1	3270 PC File Transfer Program	base

Summary of Changes

Summary of Changes
for GC28-1920-01
OS/390 Release 2

This book contains new information for OS/390 Release 2 Security Server (RACF).

Summary of Changes
for GC28-1920-00
OS/390 Release 1

This book contains information previously presented in *RACF Planning: Installation and Migration*, GC23-3736, which supports RACF Version 2 Release 2.

This book includes terminology, maintenance, and editorial changes.

Chapter 1. Planning for Migration

This chapter provides information to help you plan your installation's migration to the new release of RACF. Before attempting to migrate, you should define a plan to ensure a smooth and orderly transition. A well thought-out and documented migration plan can help minimize any interruption of service. Your migration plan should address such topics as:

- Identifying which required and optional products are needed
- Evaluating new and changed functions
- Evaluating how incompatibilities affect your installation
- Defining necessary changes to:
  - Installation-written code
  - Operational procedures
  - Application programs
  - Other related products
- Defining education requirements for operators and end users
- Preparing your staff and end users for migration, if necessary
- Acquiring and installing the latest service level of RACF for maintenance

The content and extent of a migration plan can vary significantly from installation to installation. To successfully migrate to a new release of RACF, you should start by installing and stabilizing the new RACF release without activating the new functions provided. Installing the new RACF release without initially exploiting new functions allows you to maintain a stable RACF environment. The program directory shipped with the new RACF release gives detailed information about the correct software required for installation.

When defining your installation's migration plan, you should consider the following:

- Migration
- Installation
- Customization
- Administration
- Auditing
- Operation
- Application development
- General users

Chapter 13, “Scenarios” on page 61 contains scenarios that might help you in defining your migration plan.

Migration Planning Considerations

Installations planning to migrate to a new release of RACF must consider high-level support requirements such as machine and programming restrictions, migration paths, and program compatibility.

For more information, see Chapter 4, “Planning Considerations” on page 23.

Installation Considerations

Before installing a new release of RACF, you must determine what updates are needed for IBM-supplied products, system libraries, and non-IBM products. (Procedures for installing RACF are described in the program directory shipped with the product, not in this book.)

Be sure you include the following steps when planning your pre-installation activities:

- Obtain and install any required program temporary fixes (PTFs) or updated versions of the operating system.

  Call the IBM Software Support Center to obtain the preventive service planning (PSP) upgrade for RACF. This provides the most current information on PTFs for RACF. Have RETAIN checked again just before testing RACF. Information for requesting the PSP upgrade can be found in the program directory. Although the program directory provided with the product tape contains a list of the required PTFs, the most current information is available from the support center.

- Contact programmers responsible for updating programs.

  Verify that your installation's programs will continue to run and, if necessary, make changes to ensure compatibility with the new release.

For more information, see Chapter 5, “Installation Considerations” on page 27.

Customization Considerations

In order for RACF to meet the specific requirements of your installation, you can customize function to take advantage of new support after the product is installed. For example, you can tailor RACF through the use of installation exit routines, class descriptor table (CDT) support, or options to improve performance. This book lists changes to RACF that might require the installation to tailor the product either to ensure that RACF runs as before or to accommodate new security controls that an installation requires.

For more information, see Chapter 6, “Customization Considerations” on page 35.

Administration Considerations

Security administrators must be aware of how changes introduced by a new product release can affect an installation's data processing resources. Changes to real and virtual storage requirements, performance, security, and integrity are of interest to security administrators or to system programmers who are responsible for making decisions about the computing system resources used with a program.

For more information, see Chapter 7, “Administration Considerations” on page 37.

Auditing Considerations

Auditors who are responsible for ensuring proper access control and accountability for their installation are interested in changes to security options, audit records, and report generation utilities.

For more information, see Chapter 8, “Auditing Considerations” on page 45.

Operational Considerations

The installation of a new product release might introduce changes to the operating characteristics. These changes can be in the form of changed commands, new or changed messages, or methods of implementing new functions. This book identifies those changes for which you should provide user education before running this release of the product.

For more information, see Chapter 9, “Operational Considerations” on page 49.

Application Development Considerations

Application development programmers must be aware of new functions introduced in a new release of RACF. To implement a new function, the application development personnel should read this book and the following books:

- *OS/390 Security Server External Security Interface (RACROUTE) Macro Reference*,
- *OS/390 Security Server (RACF) Data Areas*, and
- *OS/390 Security Server (RACF) Macros and Interfaces*.

To ensure that existing programs run as before, the application programmers should be aware of any changes in data areas and processing requirements. This book provides an overview of the changes that might affect existing application programs.

For more information, see Chapter 10, “Application Development Considerations” on page 51.

General User Considerations

RACF general users use a RACF-protected system to:

- Log on to the system
- Access resources on the system
- Protect their own resources and any group resources to which they have administrative authority

This book provides an overview of the changes that might affect existing procedures for general users. For more information, see Chapter 11, “General User Considerations” on page 55.

Chapter 2. Release Overview

This chapter lists the new and enhanced features of RACF for OS/390 Release 2. It also lists the support that has not been updated in the new release.

New and Enhanced Support

For OS/390 Release 2, RACF provides new and enhanced support for:

- OS/390 OpenEdition DCE
- OS/390 OpenEdition MVS
- SOMobjects for MVS, Version 1 Release 2
- SystemView for MVS
- Multisystem nodes in an RRSF network
- OS/390 enable and disable functions
- Year 2000
- NetView
- Airline Control System/MVS (ALCS/MVS)
- Information Management
- Sharing a RACF database with a VM system running RACF 1.10
- IRRUT100 support for FILE and DIRECTRY classes
- Enhanced support for coupling facility structure rebuild

OS/390 Release 2 Security Server (RACF) consists of the base code shipped with both RACF 2.2 and OS/390 Release 1 Security Server (RACF), together with PTFs that provide function enhancements. Similarly, OS/390 Release 1 Security Server (RACF) consisted of the base code shipped with RACF 2.2, together with PTFs that provided function enhancements. Therefore, the three releases differ only in the set of PTFs shipped with each. Furthermore, any PTF shipped with one of these releases can be applied to any of these releases that it was not shipped with. As a result, when you migrate to Release 2 of the OS/390 Security Server (RACF) from Release 1 of the OS/390 Security Server (RACF) or from RACF 2.2, your migration considerations depend on which PTFs are already applied on your system. If, for example, you have applied a PTF on a RACF 2.2 system for one of the functions described in this book, and you are now installing OS/390 Release 2 Security Server (RACF) on that system, you do not need to repeat migration actions you have already taken.

Figure 1 identifies function introduced after the availability of RACF 2.2 and shipped in OS/390 Release 1 Security Server (RACF).

Figure 1. Function Shipped In OS/390 Release 1 Security Server (RACF). These PTFs are also shipped in OS/390 Release 2 Security Server (RACF).

RACF Function	APAR	PTF
Support for OS/390 OpenEdition DCE	OW13895	UW90233
	OW15238 (SAF)	UW24233
Support for SOMobjects for MVS, Version 1 Release 2	OW15720	UW90266
Support for SystemView for MVS	OW18866	UW23599
SystemView panels	OW15239	UW90242

Figure 2 on page 6 identifies function introduced after the availability of OS/390 Release 1 Security Server (RACF).

Figure 2. Function Introduced After the Availability of OS/390 Release 1 Security Server (RACF). These PTFs are shipped with OS/390 Release 2 Security Server (RACF).

RACF Function	APAR	PTF
Multisystem Nodes in an RRSF Network	OW13567	UW90235
Year 2000 support	OW19251	UW90245
Enhanced support for NetView	OW19165	UW90248
Support for Airline Control System/MVS	OW19475	UW90266
Support for Information Management	OW19475	UW90266
Support for sharing a RACF database with a VM system running RACF 1.10	OW18980	UW90268

Figure 3 identifies function introduced in OS/390 Release 2 Security Server (RACF).

Figure 3. Function Introduced In OS/390 Release 2 Security Server (RACF). These PTFs are shipped with OS/390 Release 2 Security Server (RACF).

RACF Function	APAR	PTF
Support for OS/390 enable and disable functions	OW19377	UW90250
Support for OS/390 OpenEdition MVS	OW19376	UW90247

Figure 4 identifies function not shipped in OS/390 Release 2 Security Server (RACF), but available via PTF.

Figure 4. Function Not Shipped In OS/390 Release 2 Security Server (RACF). This function is available via PTF on RACF 2.2, OS/390 Release 1 Security Server (RACF), and OS/390 Release 2 Security Server (RACF)

RACF Function	APAR	PTF
IRRUT100 updates for FILE and DIRECTRY classes	OW20759	UW90296
Enhanced support for coupling facility structure rebuild	OW19407	UW90293

OS/390 OpenEdition DCE

The OS/390 OpenEdition DCE feature integrates the Open Software Foundation Distributed Computing Environment technologies with the MVS/ESA operating system. DCE technology on MVS/ESA enables MVS participation in a heterogeneous distributed computing environment. The OS/390 OpenEdition DCE feature provides support for industry-standard mechanisms for application distribution while considering the current host application development environment.

RACF establishes a *cross-linking* of identity between a RACF user ID and a DCE user identity *(principal)*. This cross-linking allows DCE application servers that reside on MVS to use the access control and auditing mechanisms provided by RACF in the MVS environment. The cross-linking also provides information that

OS/390 OpenEdition DCE single signon support uses to sign in an authenticated OS/390 user to DCE.

The RACF support for OS/390 OpenEdition DCE includes:

- The DCE segment, which contains DCE information associated with a RACF user
- The KEYSMSTR class, which holds a key to encrypt the DCE password
- The DCEUUIDS class, which is used to define the mapping between a user's RACF user ID and the corresponding DCE principal UUID
- Callable services that:
  - Check a user's authority to a RACF resource
  - Set or retrieve fields from a user profile DCE segment
  - Set or retrieve a DCE password
  - Determine the identity of a DCE client
- Enhancements to RACF commands to allow users to create, update and display information in the DCE user profile segment:
  - ADDUSER
  - ALTUSER
  - LISTUSER
- Enhancements to RACF utilities:
  - SMF data unload utility
  - Database unload utility
  - Remove ID utility
- Enhancements to the ACEE to identify a DCE client
- Enhancements to RACF ISPF panels for the DCE user profile segment

OS/390 OpenEdition DCE provides two utilities to administer DCE information in the RACF database and to create cross-linking information between the RACF user database and the DCE principal registry:

- MVSIMPT
- MVSEXPT

For more information on these utilities, see *OpenEdition DCE Administration Guide*.

RACF interoperation with DCE requires the following software:

- OpenEdition/MVS Release 3 (HOM1130) plus APAR OW15865
- C Run Time Library (JMWL550) plus APAR PN75309

To enhance the security of DCE passwords stored in the RACF database, you might want to use an encryption product. You are encouraged to consider installing the IBM Integrated Cryptographic Service Facility (ICSF) Version 1 Release 2 on your MVS operating system. This product provides DES encryption-level protection.

For an overview of DCE technology and terminology, see *DCE: Understanding the Concepts*.

OS/390 OpenEdition

OS/390 Release 2 OpenEdition adds new capabilities for which RACF provides support.

Authorizing and Auditing Server Access to the CCS and WLM Services

OS/390 Release 2 OpenEdition adds the capability to check whether servers are authorized to use the console communications service (CCS) and the workload manager (WLM) service. RACF provides support for this capability by determining whether the server identity has authority to the service, and by auditing requests for access to these services.

RACF provides two new audit function codes for these services. The auditing is based on the existing PROCESS class.

Auditing the Passing of Access Rights

OS/390 Release 2 OpenEdition implements the passing of access rights from one process to another. A sending process opens a file and passes the open file descriptor to a receiving process via a UNIX domain socket connection. RACF writes SMF type 80 records when:

- The access rights are passed by the sending process.
- The access rights are received by the receiving process.
- The access rights are discarded by the receiving process without being received.

RACF provides a new event code and 3 new audit function codes for these SMF records. Auditing is based on the existing PROCACT class.

SOMobjects for MVS

RACF provides support for Version 1 Release 2 of SOMobjects for MVS. A client application running in an OS/2, AS/400, or MVS environment requesting distributed SOM (DSOM) services can have those services run in an MVS server. To support the use of remote objects with SOMobjects for MVS, RACF does the following:

- Authenticates the user as a valid and correct user through the presentation of a password
- Verifies the user's access to use the requested server
- Verifies the server's access to use the method within the specified class
- Verifies that only approved servers can register with the SOMojbects for MVS server daemon, preventing unauthorized users from starting trojan horse servers

SystemView for MVS

SystemView for MVS consists of programs that run on the user's workstation and programs that run on MVS. SystemView for MVS displays a *Launch window* that contains a customized task tree. This *task tree* represents systems management programs, or applications, to which the workstation user can get access. The information needed by the SystemView for MVS client code running in the workstation is created and stored on the MVS-based SystemView server system,

so that the user's information can be customized independently of the user's workstation type.

The SystemView Launch window lets users log on once, authenticating with their RACF password, and then get access to applications that SystemView for MVS supports by selecting an application from their customized task tree, without needing to specify a user ID and password again.

With this support, security administrators can:

- Define applications enabled for the SystemView for MVS Launch window to RACF
- Authorize SystemView for MVS users to get access to these defined applications through the Launch window
- Define logon script and parameter information for the SystemView for MVS Launch window

A new RACF class, SYSMVIEW, allows the RACF administrator to control access to SystemView for MVS applications. This new class also enables the defining of customized sign-on script and parameter information used by the SystemView for MVS user. See *SystemView for MVS Up and Running!* for information about SystemView for MVS and the Launch window.

Multisystem Nodes in an RRSF Network

The RACF remote sharing facility (RRSF) has been enhanced to provide multisystem node support, allowing you to configure MVS system images that share a RACF database into one *multisystem RRSF node*. You designate one of the MVS system images to be the *main system*. The main system receives most of the RRSF communications sent to the node. The other systems are known as *non-main systems*.

Main systems in a multisystem RRSF node can send directed commands and password changes to main systems on remote multisystem RRSF nodes, and to single-system nodes. In addition, when main systems receive requests from remote systems (main or non-main), they send output and notifications back to the system that originated the request.

Non-main systems in a multisystem RRSF node can send directed commands and password changes to main systems on remote multisystem RRSF nodes, and to single-system RRSF nodes. They cannot send RRSF requests to other remote non-main systems, or to other local systems (non-main or main).

Most RRSF communications sent to the multisystem RRSF node are received by the main system, including:

- All commands directed to the multisystem node
- All RACLINK requests sent to the multisystem node
- All password changes sent to the multisystem node
- All output and notifications from automatically directed commands

The following types of RRSF communications can be received by any system in a multisystem node:

- Output and notifications from commands that were directed via the AT or ONLYAT keywords. These are returned to the system on which the directed command was issued.
- Notifications from RACLINK commands. These are returned to the system on which the RACLINK command was issued.
- Output from password changes when automatic password direction is used. These are returned to the system on which the password was changed.

Although the member systems of a multisystem RRSF node do not communicate with each other via RRSF functions, each system in the multisystem node must issue TARGET commands describing the other systems in the multisystem node. RACF needs this TARGET information if you reconfigure the multisystem node with a different main system. The systems can share a common RACF parameter library that contains all of the TARGET commands required.

It is possible to define a multisystem node that contains only one system. This configuration might be useful as a migration path.

The RACF support for multisystem RRSF nodes includes:

- Enhancements to the TARGET command to allow system programmers to configure multisystem RRSF nodes
- Enhancements to the RESTART command to allow operators to restart connections to systems in multisystem RRSF nodes
- A new naming convention for the workspace data sets used by RACF for RRSF communications
- A new connection state, the *defined* state

For more information on multisystem RRSF nodes, see *OS/390 Security Server (RACF) System Programmer's Guide*.

OS/390 Enable and Disable Functions

OS/390 provides a registration service to enable and disable features. RACF for OS/390 Release 2 supports this enable and disable function.

Entries in the IFAPRD*xx* parmlib member specify which features are enabled and disabled. When you install OS/390 Release 2, make sure that an entry exists in IFAPRD*xx* to enable RACF. If RACF is not enabled, RACF initialization will not complete, and RACF will not provide security for the system.

For more information, see “Enabling RACF” on page 27.

Year 2000

RACF dates are 3-byte packed decimal fields in the form *yydddF*. This format does not allow the first two characters of the year to be specified. In the past it has been acceptable to assume that the date is in the twentieth century, and that the first two characters of the year are `'19'`. However, as the end of the twentieth century approaches, support is required for dates where the first two characters of the year are `'20'`.

RACF now considers a date with a *yy* value of 70 or less to be in the year 20*yy*, and a date with a *yy* value greater than 70 to be in the year 19*yy*. RACF provides

the IRRDCR00 module to allow customers to convert a 3-byte packed decimal date to a 4-byte packed decimal date, using RACF's interpretation of the *yy* value. For more information on IRRDCR00, see “Year 2000 Support” on page 51.

NetView

RACF has added the NGMFVSPN field to the NETVIEW segment of the RACF user profile for future use by the NetView Graphic Monitor Facility. To support this new field, a new keyword has been added to the RACF ADDUSER and ALTUSER commands, and the RACF panels have been enhanced.

Airline Control System/MVS (ALCS/MVS)

RACF provides a new class, ALCSAUTH, to support ALCS/MVS Version 2 Release 2.

Information Management

The maximum length of resource names for the INFOMAN and GINFOMAN classes has increased from 39 to 44.

Sharing a RACF Database with a VM System Running RACF 1.10

RACF provides enhancements to allow systems to share a RACF database with a VM system running RACF 1.10. The enhancements include:

- Four new classes: VMPOSIX, FILE, DIRECTRY, and SFSCMD.
- Support for the OVM segment in the RACF user and group profiles. This support allows a system running OS/390 Release 2 Security Server (RACF) to share a RACF database with a system running RACF 1.10 for VM. But this support *does not* allow administration of the OVM segment using the RACF commands from OS/390 Release 2 Security Server (RACF). You can administer the OVM segments only from a RACF 1.10 for VM system.
- Enhancements to the RACF database unload utility (IRRDBU00) to support unloading data from the OVM segments in the user and group profiles.
- Enhancements to the RACF SMF data unload utility (IRRADU00) to support unloading data from audit records created on RACF 1.10 for VM. This support allows RACF 1.10 for VM audit records to be processed by OS/390 Release 2 Security Server (RACF).

IRRUT100 Support for the FILE and DIRECTRY classes

PTF UW90296 updates the IRRUT100 utility to find FILE and DIRECTRY profiles that have a second-level qualifier matching the input user name.

Enhanced Support for Coupling Facility Structure Rebuild

PTF UW90293 significantly enhances RACF's support of coupling facility structure rebuild. Enhancements include:

- Improved performance in the rebuild of RACF structures
- Support of the LOC=OTHER parameter for operator-driven rebuilds
- Support of REBUILDPERCENT as specified in the coupling facility resource management policy

The PTF must be applied to all systems in the sysplex in order for these enhancements to take effect. However, systems with and without the PTF applied can coexist in the sysplex, and there is no requirement to IPL all systems in the sysplex when the PTF is applied.

Note: PTF UW90293 is not shipped with OS/390 Release 2 Security Server (RACF). You must obtain it and install it after you install OS/390 Release 2 Security Server (RACF).

Function Not Upgraded

Figure 5 identifies function that has not been updated for OS/390 Release 2.

Figure 5. Function Not Upgraded

Function	Description
Report writer	The RACF report writer has not been enhanced since RACF 1.9.2, and will not be enhanced in the future. Although it can process the SMF records created by RACF on OS/390 Release 2, it cannot report on any new function, except for certain RACF enhancements automatically handled by the report writer, including: • SETROPTS options that affect new RACF classes • Access successes or failures for resources in new RACF classes Installations using the RACF report writer function must change to another reporting package in order to obtain full reports from RACF SMF records. The RACF SMF data unload utility, IRRADU00, has been enhanced to unload SMF data for new functions, and can be used as a vehicle for creating a reporting function.

Chapter 3. Summary of Changes to RACF Components for OS/390 Release 2

This chapter summarizes the new and changed components of OS/390 Release 2 Security Server (RACF). It includes summary charts for changes to the RACF:

- Class descriptor table (CDT)
- Commands
- Data Areas
- Exits
- Macros
- Messages
- Panels
- Publications Library
- Routines
- SYS1.SAMPLIB
- Templates
- Utilities

Class Descriptor Table (CDT)

Figure 6 lists the new classes provided in the IBM-supplied class descriptor table (ICHRRCDX). For each class, a corresponding entry has been added to the IBM-supplied router table (ICHRFR0X). The class names (when the classes have profiles) are general-use programming interfaces (GUPI) for ICHEINTY and RACROUTE.

For more information, see *OS/390 Security Server (RACF) Macros and Interfaces*.

Figure 6 (Page 1 of 2). New Classes

Class Name	Description	Support
ALCSAUTH	This class contains general resource profiles for functions and facilities of the Airline Control System (ALCS) Version 2 Release 2 product, and optionally for functions and facilities of customer-written applications that run under ALCS Version 2 Release 2.	Airline Control System/MVS (ALCS/MVS)
CBIND	This class controls the client's ability to bind to the SOMobjects for MVS server. The naming convention for profiles in the CBIND class is: `SOM.DSOM.`*`server-name`*	SOMobjects for MVS
DCEUUIDS	Discrete profiles in this class define the mapping between a user's RACF user ID and the corresponding DCE principal UUID. Profile names can be in either of the following forms: *`principal_uuid`* *`home_cell_uuid.principal_uuid`*	OS/390 OpenEdition DCE
DIRECTRY	This class controls protection of shared file system (SFS) directories on VM.	RACF 1.10 for VM

Figure 6 (Page 2 of 2). New Classes

Class Name	Description	Support
FILE	This class controls protection of shared file system (SFS) files on VM.	RACF 1.10 for VM
KEYSMSTR	This class holds a key to encrypt DCE passwords stored in the RACF database. The profile in this class is named: `DCE.PASSWORD.KEY` The profile contains an SSIGNON segment that holds either the masked or encrypted value for the key that is used to encrypt DCE passwords.	OS/390 OpenEdition DCE
SERVER	This class controls a server's ability to register with the SOM daemon. The naming convention for profiles in the SERVER class is: `SOM.DSOM.`*`server-name`*	SOMobjects for MVS
SFSCMD	This class controls the use of shared file system (SFS) administrator and operator commands on VM.	RACF 1.10 for VM
SOMDOBJS	This class controls a client's ability to invoke a method in a class. The naming convention for profiles in the SOMDOBJS class is: *`class.method-name`*	SOMobjects for MVS
SYSMVIEW	This class lets the RACF administrator control access to SystemView for MVS applications via the SystemView for MVS launch window. It also enables the defining of customized sign-on script and parameter information used by the SystemView for MVS user.	SystemView
VMPOSIX	This class contains profiles used by OpenEdition VM.	RACF 1.10 for VM

Figure 7 lists classes for which there are changes.

Figure 7. Changed Classes

Class Name	Description	Support
INFOMAN GINFOMAN	The maximum length of resource names has increased from 39 to 44.	Information Management
JCICSJCT KCICSJCT	The maximum length of profile names has increased from 16 to 17.	CICS

Commands

Figure 8 lists the changes to RACF commands for OS/390 Release 2.

For more information, see *OS/390 Security Server (RACF) Command Language Reference*.

Figure 8. Changes to RACF Commands

Command	Description	Support
all	If an attempt is made to invoke a RACF command when RACF is not enabled, RACF issues message IRR418I, and the command is not processed.	OS/390 Enable/Disable
ADDUSER ALTUSER	These commands accept the new NGMFVSPN subkeyword on the NETVIEW keyword for future use by the NetView Graphic Monitor Facility. The ALTUSER command also accepts the new NONGMFVSPN subkeyword on the NETVIEW keyword.	NetView
ADDUSER ALTUSER LISTUSER	A new keyword, DCE, allows a security administrator to specify, update, and list information that RACF stores in the DCE segment of a user's profile. Subkeywords of the DCE keyword allow a security administrator to specify, update, and list: • Whether OS/390 OpenEdition DCE is to log a RACF user into OS/390 OpenEdition DCE automatically • The DCE principal name defined for a RACF user in the DCE registry • The DCE cell name defined for a RACF user • The DCE universal unique identifier (UUID) for the cell that a RACF user is defined to • The DCE universal unique identifier (UUID) of a DCE principal	OS/390 OpenEdition DCE
RALTER RDEFINE	A new keyword, SVFMR, allows a security administrator to create and alter profiles within the SYSMVIEW class for SystemView for MVS applications. Subkeywords of the SVFMR keyword allow a security administrator to specify: • The name of a list of default logon scripts associated with the application • The name of a parameter list associated with the application	SystemView
RESTART	A new keyword, SYSNAME, allows an operator to restart the connections with all systems or a specified system on a multisystem node.	Multisystem RRSF nodes
RLIST	A new keyword, SVFMR, allows profiles in the SYSMVIEW class to be listed.	SystemView
TARGET	A new keyword, SYSNAME, identifies which system on a multisystem RRSF node the command pertains to. A new keyword, MAIN, identifies the system named on the SYSNAME keyword as the main system in a multisystem RRSF node. The information displayed when you specify the LIST keyword can include information about the systems that make up a multisystem node.	Multisystem RRSF nodes

Data Areas

Figure 9 lists changed general-use programming interface (GUPI) data areas for SAF to support RACF for OS/390 Release 2.

Figure 9. Changes to SAF GUPI Data Areas

Data Area	Description	Support
ACEE	This data area has been enhanced to identify a DCE client.	OS/390 OpenEdition

Figure 10 lists changed product-sensitive programming interface (PSPI) data areas for for RACF.

Figure 10. Changes to PSPI Data Areas

Data Area	Description	Support
AFC	This data area, which defines audit function codes, has been updated to add two new audit function codes for OS/390 OpenEdition auditing of the console communications service (CCS) and workload manager (WLM) service, and three new audit function codes for OS/390 OpenEdition auditing of the passing of access rights from one process to another.	OS/390 OpenEdition
AFC	This data area, which defines audit function codes, has been updated to add a new audit function code for OS/390 OpenEdition DCE support.	OS/390 OpenEdition DCE
COMP	This data area defines the SAF/RACF parameter list format for RACF services for OpenEdition MVS. It defines a common part for all services and a variable part for each service or set of related services. This data area is updated to support OpenEdition DCE.	OS/390 OpenEdition DCE
FC	This data area defines the function codes for callable services. It is updated to support OpenEdition DCE.	OS/390 OpenEdition DCE
SMFR9	This data area documents the event codes for the SMF type 80 record. It is updated to add the new event code 65 used to audit the passing of access rights.	OS/390 OpenEdition

Exits

Figure 11 lists changes to installation exits for OS/390 Release 2. These changes are product-sensitive programming interfaces (PSPI).

Figure 11. Changed Exits for RACF		
Exit	**Description**	**Support**
ICHRCX01 ICHRCX02	For unauthenticated client ACEEs, the RACROUTE REQUEST=AUTH preprocessing and postprocessing exits are invoked for both the client ACEE and the server ACEE. For more information, see “Effects of OS/390 OpenEdition DCE Support on ICHRCX01, ICHRCX02, and IRRSXT00” on page 35.	OS/390 OpenEdition DCE
ICHRDX01	Processing of a RETPD value specified via the RACROUTE REQUEST=DEFINE preprocessing exit has changed. For more information, see “RACROUTE REQUEST=DEFINE Preprocessing Exit (ICHRDX01)” on page 36.	APAR OW13967
IRRSXT00	For the R_dceinfo and R_dceruid callable services: • IRRSXT00 must be capable of executing in either problem or supervisor state. • IRRSXT00 must not expect to receive control in a system storage protection key (0-7).	OS/390 OpenEdition DCE

Macros

Figure 12 lists changes to RACF macros for OS/390 Release 2. These changes are general-use programming interfaces (GUPI).

Figure 12. Changed Macros for RACF		
Macro	**Description**	**Support**
ICHEINTY	The ICHEINTY macro can be used to rename profiles in the FILE and DIRECTRY classes. The existing keywords RENAME, NEWNAME, and NEWNAMX can now be used to rename profiles when specifying CLASS=FILE or CLASS=DIRECTRY.	RACF 1.10 for VM
RACROUTE	The RACROUTE REQUEST=DEFINE macro can be used to rename resources in the new FILE and DIRECTRY classes. The existing keywords NEWNAME and NEWNAMX can now be used to rename resources when specifying CLASS=FILE or CLASS=DIRECTRY. For more information, see *OS/390 Security Server External Security Interface (RACROUTE) Macro Reference*.	RACF 1.10 for VM

Messages

The messages that have been added or changed in RACF for OS/390 Release 2 are listed below. Compare the message identifiers and the corresponding message text with any automated operations procedures your installation uses to determine whether updates are required.

New Messages

The following messages are added:

RACF Initialization Messages: ICH562I

RACF Processing Messages: IRR418I

Dynamic Parse (IRRDPI00 Command) Messages: IRR52152I

RACF Database Split/Merge Utility (IRRUT400) Messages: IRR65038I

Messages Issued by the RACF Subsystem: IRRB022I, IRRB077I, IRRB078I, IRRB079I, IRRB080I, IRRB081I, IRRB082I

RRSF Handshaking Messages: IRRI014I, IRRI015I

TARGET Command Messages: IRRM026I, IRRM027I, IRRM028I, IRRM029I, IRRM030I, IRRM031I, IRRM032I, IRRM033I, IRRM034I, IRRM035I, IRRM036I, IRRM037I, IRRM038I, IRRM039I, IRRM040I, IRRM041I, IRRM054I

RACF Operational Modes and Coupling Facility Related Messages: IRRX020I, IRRX021

Changed Messages

The following messages are changed:

RDEFINE Command Messages: ICH10301I

RACF Miscellaneous Messages: ICH70001I

VERIFY and VERIFYX Messages: IRR008I

Messages Issued by the RACF Subsystem: IRRC022I, IRRC024I, IRRC026I, IRRC032I, IRRC033I

RRSF Handshaking Messages: IRRI000I, IRRI001I, IRRI004I, IRRI005I, IRRI011I, IRRI012I, IRRI013I

TARGET Command Messages: IRRM005I, IRRM007I, IRRM008I, IRRM009I, IRRM010I, IRRM011I, IRRM013I, IRRM014I, IRRM015I, IRRM016I, IRRM017I, IRRM018I, IRRM020I, IRRM021I, IRRM022I, IRRM023I, IRRM049I, IRRM050I, IRRM052I

RRSF Connection Receive Transaction Program Messages: IRRN000I, IRRN009I, IRRN020I, IRRN021I

RRSF Output Handling Task Messages: IRRR015I

RACF Operational Modes and Coupling Facility Related Messages: IRRX001I, IRRX003A, IRRX017I

Panels

Figure 13 lists RACF panels that are changed.

Figure 13. Changed Panels for RACF

Panel	Description	Support
ICHP41I ICHP42I	Existing panels for user administration of the NETVIEW segment have been updated to allow a user to add, change, or delete the NGMFVSPN field.	NetView

Publications Library

Figure 14 lists changes to the OS/390 Security Server (RACF) publications library.

Figure 14. Changes to the RACF Publications Library

Publication	Description	Support
IBM Online Library Productivity Edition: OS/390 Security Server (RACF) Information Package	This softcopy collection kit has been renamed from *IBM Online Library Productivity Edition: RACF Information Package*, and the price has been lowered when ordered as a feature of OS/390 or RACF.	

Routines

Figure 15 lists a new routine for RACF. The interface to this routine is a general-use programming interface (GUPI).

Figure 15. Changes to Routines

Routine	Description	Support
IRRDCR00	The date conversion routine converts a 3-byte packed decimal date in the form *yydddF* to a 4-byte packed decimal date in the form: 00*yydddF* if *yy* >= 71 01*yydddF* if *yy* < 71 For more information, see *OS/390 Security Server (RACF) Macros and Interfaces*.	Year 2000

SYS1.SAMPLIB

Figure 16 identifies changes to RACF members of SYS1.SAMPLIB.

Figure 16. Changes to SYS1.SAMPLIB

Member	Description	Support
IRRADULD	This member has been updated with the SMF type 80 record for the new event code 65.	OS/390 OpenEdition
IRRADULD	This member has been updated to support RACF 1.10 for VM audit records.	RACF 1.10 for VM
IRRADUTB	This member has been updated with the SMF type 80 record for the new event code 65.	OS/390 OpenEdition
IRRADUTB	This member has been updated to support RACF 1.10 for VM audit records	RACF 1.10 for VM
RACDBULD	The load statement for the NETVIEW segment data has been updated to include the NGMFVSPN field.	NetView
RACDBULD	This member has been updated to support the OVM segment in user and group profiles.	RACF 1.10 for VM
RACDBULD	This member has been updated to support the DCE segment.	OS/390 OpenEdition DCE
RACDBULD	This member has been updated to support the SVFMR segment.	SystemView for MVS
RACDBUTB	The create table statement for the NETVIEW segment has been updated to include the NGMFVSPN field.	NetView
RACDBUTB	This member has been updated to support the OVM segment in user and group profiles.	RACF 1.10 for VM
RACDBUTB	This member has been updated to support the DCE segment.	OS/390 OpenEdition DCE
RACDBUTB	This member has been updated to support the SVFMR segment.	SystemView for MVS
RACTABLE	Previous references to ASMHCL have been modified to reference HLASMCL.	

Templates

Figure 17 lists changes to RACF database templates. All of the fields identified in Figure 17 are general-use programming interfaces (GUPI) for ICHEINTY and RACROUTE REQUEST=EXTRACT.

Figure 17. Changes to Templates

Template	Description of Change	Support
General	A new SVFMR segment provides the following information: *Field* *Description* SCRIPTN Script name PARMN Parameter list name	SystemView for MVS
Group	A new OVM segment provides OpenEdition for VM information associated with a group. The segment provides the following information: *Field* *Description* GID GID binary	RACF 1.10 for VM
User	A new DCE segment provides DCE information associated with a RACF user. The segment provides the following information: *Field* *Description* UUID User's DCE principal's UUID DCENAME User's DCE principal name HOMECELL Home cell for the user HOMEUUID Home cell UUID DCEFLAGS User flags DPASSWDS Current DCE password DCEENCRY Password masking/encryption key	OS/390 OpenEdition DCE
User	A new 8-character field, NGMFVSPN, has been added to the NETVIEW segment. This field is reserved for future use by the NetView Graphic Monitor Facility.	NetView
User	A new OVM segment provides OpenEdition for VM information associated with a user. The segment provides the following information: *Field* *Description* UID UID binary HOME Home path PROGRAM Initial program FSROOT File system root	RACF 1.10 for VM

Utilities

Figure 18 lists changes to RACF utilities for OS/390 Release 2.

Figure 18. Changes to Utilities

Utility	Description of Change	Support
IRRADU00	The SMF data unload utility has been updated to support unloading data from audit records created on a system running RACF 1.10 for VM. This support allows RACF 1.10 for VM audit records to be processed by OS/390 Security Server (RACF).	RACF 1.10 for VM
IRRDBU00	The RACF database unload utility creates a new record type 0290 for the user DCE data.	OS/390 OpenEdition DCE
IRRDBU00	The RACF database unload utility creates two new record types: • Record type 0130 for the group data for OpenEdition VM • Record type 02A0 for the user data for OpenEdition VM	RACF 1.10 for VM
IRRDBU00	The RACF database unload utility creates a new record type 0550 for the general resource data for SystemView for MVS.	SystemView for MVS
IRRDUB00	The RACF database unload utility creates a new field at the end of the NETVIEW segment record for the user profile (record type 0280) for the NGMFVSPN field.	NetView
IRRRID00	The RACF remove ID utility has been enhanced to search profiles defined to the DCEUUIDS class when removing a user ID.	OS/390 OpenEdition DCE
IRRUT100	With PTF UW90296, the RACF cross-reference utility has been updated to find FILE and DIRECTRY profiles that have a second-level qualifier matching the input user name. ┌ general-use programming interface The utility produces a new record type (X'18') for a qualifier of a FILE or DIRECTRY general resource profile. └ End of general-use programming interface	RACF 1.10 for VM
BLKUPD ICHDSM00 ICHRSMF0 IRRBRW00 IRRDBU00 IRRDPI00 IRRRID00 IRRUT100 IRRUT200 IRRUT400	If an attempt is made to invoke one of these utilities when RACF is not enabled, the utility issues message IRR418I and return code X'20'. The utility does not continue. For more information, see “Enabling RACF” on page 27.	OS/390 Enable/Disable

Chapter 4. Planning Considerations

This chapter describes the following high-level planning considerations for customers upgrading to Security Server (RACF) Release 2 from Security Server (RACF) Release 1:

- Migration strategy
- Migration paths
- Hardware requirements
- Software requirements
- Compatibility

Migration Strategy

The recommended steps for migrating to a new release of RACF are:

1. Become familiar with the release documentation.
2. Develop a migration plan for your installation.
3. Install the product using the program directory shipped with the product.
4. Use the new release before initializing major new function.
5. Customize the new function for your installation.
6. Exercise the new function.

Migration Paths for OS/390 Release 2 Security Server (RACF)

- From OS/390 Release 1 Security Server (RACF) or RACF 2.2

  If you are an OS/390 Release 1 Security Server (RACF) or RACF 2.2 customer, you can migrate to OS/390 Release 2 Security Server (RACF) if you meet the OS/390 release requirements and the other software requirements. (OS/390 Release 1 Security Server (RACF) and RACF 2.2 are functionally equivalent.)

- From RACF 1.9.2 or RACF 2.1

  If you are a RACF 1.9.2 or 2.1 customer, you can migrate to OS/390 Release 2 Security Server (RACF) if you meet the OS/390 release requirements and the other software requirements. If you have RACF 2.1 installed, in addition to this book you should read:

  – *OS/390 Security Server (RACF) Planning: Installation and Migration* for OS/390 Release 1.

  If you have RACF 1.9.2 installed, in addition to this book you should read:

  – *OS/390 Security Server (RACF) Planning: Installation and Migration* for OS/390 Release 1, and

  – *RACF Planning: Installation and Migration* for RACF 2.1.

- From RACF 1.9

  If you are a RACF 1.9 customer, you can migrate to OS/390 Release 2 Security Server (RACF) if you are running with the restructured database and meet the OS/390 release requirements and the other software requirements. If your database is not restructured, you must restructure it and perform appropriate testing of any installation-supplied code that uses ICHEINTY or

RACROUTE REQUEST=EXTRACT,TYPE=EXTRACT or TYPE=REPLACE before installing OS/390 Release 2 Security Server (RACF). In addition to this book you should read:

- *OS/390 Security Server (RACF) Planning: Installation and Migration* for OS/390 Release 1,
- *RACF Planning: Installation and Migration* for RACF 2.1, and
- *RACF Migration and Planning* for RACF 1.9.2.

- From RACF releases prior to 1.9

  If you are on a RACF release prior to 1.9, you must install RACF 1.9, restructure your database, and perform appropriate testing of any installation-supplied code that uses ICHEINTY or RACROUTE REQUEST=EXTRACT,TYPE=EXTRACT or TYPE=REPLACE. (Note, however, that RACF 1.9 is no longer available. If you do not already have RACF 1.9, contact your IBM representative for assistance.) Then, if you meet the OS/390 release requirements and the other software requirements, you can install OS/390 Release 2 Security Server (RACF). In addition to this book you should read:

  - *OS/390 Security Server (RACF) Planning: Installation and Migration* for OS/390 Release 1,
  - *RACF Planning: Installation and Migration* for RACF 2.1,
  - *RACF Migration and Planning* for RACF 1.9.2, and
  - *RACF Migration and Planning* for RACF 1.9.

Hardware Requirements

OS/390 Release 2 Security Server (RACF) does not require any specific hardware support. It runs on all hardware supported by OS/390 Release 2. However, data sharing mode in the Parallel Sysplex requires a coupling facility configured for RACF's use.

For systems in a multisystem RRSF node, we recommend placing:

- All workspace data sets on shared DASD and in a shared catalog
- All RRSFLIST data sets on shared DASD
- One RACF parameter library on shared DASD to be used by all systems

RACF cannot ensure that the systems in a multisystem RRSF node share a RACF database. The system programmer must ensure that the RACF database for a multisystem RRSF node is on shared DASD and shared by the systems in the multisystem node.

Software Requirements

Figure 19 summarizes the software requirements for the new function provided by OS/390 Release 2 Security Server (RACF). For an overview of the function, including the PTFs that provide the function, see Chapter 2, “Release Overview” on page 5.

Figure 19. Software Requirements for New Function	
Function	**Software Requirements**
OS/390 OpenEdition DCE interoperability support	OpenEdition/MVS Release 3 plus APAR OW15865 (PTF UW23684) C Run Time Library plus APAR PN75309 (PTF UN90158)
SOMobjects for MVS support	Version 1 Release 2 of SOMobjects for MVS

Compatibility

This section describes considerations for compatibility between OS/390 Release 2 Security Server (RACF) and OS/390 Release 1 Security Server (RACF).

Compatibility Considerations for Remote Sharing

Multisystem node support requires a change to the names of the workspace data sets used by the RACF remote sharing facility (RRSF). If your installation has configured an RRSF network, drain your workspace data sets or rename them to the new names before you install OS/390 Release 2 Security Server (RACF). If you don't, requests that are in the old workspace data sets will be ignored after you install OS/390 Release 2 Security Server (RACF). See “Considerations for RRSF Networks” on page 27 for more information.

Chapter 5. Installation Considerations

This chapter describes changes of interest to the system programmer installing OS/390 Release 2 Security Server (RACF):

- Enabling RACF
- Considerations for RRSF networks
- Virtual storage considerations
- Customer additions to the CDT
- Templates

Enabling RACF

When you install OS/390 Release 2, make sure that RACF is enabled. If it is not, RACF initialization does not complete, message IFA104I is issued, and RACF does not provide security for the system.

At install time, to enable RACF, an entry must exist in the IFAPRD*xx* member pointed to by the PROD= parameter in the IEASYS*xx* member of SYS1.PARMLIB. If you order RACF as part of the Security Server feature in OS/390 release 2, the IFAPRD*xx* entry should look like this:

```
PRODUCT OWNER('IBM CORP')
        NAME('OS/390')
        FEATURENAME('Security Server')
        ID(5645-001)
        VERSION(*)
        RELEASE(*)
        MOD(*)
        STATE(ENABLED)
```

If you make changes to this member, you must re-IPL the system for the changes to take effect. RACF does not respond to changes made via the MVS SET PROD command.

For more information on enabling and disabling RACF, see *OS/390 Security Server (RACF) System Programmer's Guide*, or the program directory shipped with the product. For general information on enabling products, see *OS/390 MVS Product Management*.

Considerations for RRSF Networks

OS/390 Release 2 Security Server (RACF) includes support for multisystem nodes in RRSF networks. (For a description of this support, see “Multisystem Nodes in an RRSF Network” on page 9.) This support required a change to the naming convention for the remote sharing workspace data sets. The naming convention for the workspace data sets created on a node as a result of a TARGET LOCAL command is now:

prefix.sysname.ds_identity

where:

prefix	Is a value you specify with the PREFIX keyword on the TARGET command
sysname	Is the system name. This name must match the value in the CVTSNAME field for the system it identifies.
ds_identity	Is either INMSG or OUTMSG

The naming convention for the workspace data sets for remote connections is now:

prefix.local_luname.remote_luname.ds_identity

where:

prefix	Is a value you specify with the PREFIX keyword on the TARGET command
local_luname	Is the LU name of the local node
remote_luname	Is the LU name of the remote node
ds_identity	Is either INMSG or OUTMSG

If your installation has configured an RRSF network, you could lose requests that are in your existing workspace data sets when you install multisystem RRSF node support. To avoid losing requests, follow these steps before you install multisystem RRSF node support on a system in an RRSF network:

1. Warn users of this migration. Start this process at a time appropriate for your installation. Pay particular attention to the effects of locking the RACF database (step 3). Updates to a locked RACF database are not allowed, and result in ABEND483 or ABEND485. See *OS/390 Security Server (RACF) System Programmer's Guide* for information on locking a database.
2. On the system on which you are installing multisystem node support, issue TARGET DORMANT commands for all remote nodes, and wait until their INMSG workspace data sets have drained. You can use a TARGET LIST command for each specific remote node to verify that the INMSG file is empty. As a result of this step:
   - Future requests from remote nodes are not received. They queue up in the OUTMSG files for this system on the remote nodes.
   - Pending requests from remote nodes are processed before you lock the RACF database.
3. Use the IRRUT400 utility to lock the RACF database. Specify `PARM='LOCKINPUT'` with no OUTDD statements in the JCL. The utility gives a return code of 4, but locks the database. Locking the database prevents the database from getting out of synchronization with other RACF databases in the RRSF network during the install.

   It is important to completely finish step 2 before locking the database. Otherwise, pending update requests already received from remote nodes will result in abends, and could cause the out-of-sync condition that this step is attempting to prevent.
4. Install RACF.
5. Stop the RACF subsystem address space.

   If the INMSG and OUTMSG workspace data sets are empty at this time, new workspace data sets can be allocated that follow the new naming convention. You can preallocate these data sets, or let RACF allocate them for you. See

the description of the TARGET command in *OS/390 Security Server (RACF) Command Language Reference* for details.

If any of the INMSG or OUTMSG workspace data sets are not empty, you should rename them to follow the new naming convention. For an example of JCL to perform this task, see Figure 20 on page 30.

6. Restart the RACF subsystem address space to pick up the renamed workspace data sets and the updated code.
7. Use the IRRUT400 utility to unlock the RACF database. Specify `PARM='UNLOCKINPUT'` with no OUTDD statements in the JCL. For more information on IRRUT400, see *OS/390 Security Server (RACF) System Programmer's Guide*.

As long as all the RRSF nodes in an RRSF network are single-system RRSF nodes, nodes with multisystem node support installed can continue to communicate with nodes that do not have the support installed. However, the multisystem node support must be installed on each RRSF node in an RRSF network before a multisystem node can be defined in the network. If you attempt to define a multisystem node and multisystem node support has not been installed on each node in the network, RACF issues an error message.

```
//*****************************************************************//
//*                                                                 *//
//* RRSFALTR:                                                       *//
//*                                                                 *//
//* IDCAMS JOB to rename the workspace data sets when installing    *//
//* PTF UW90235 (multisystem node support)                          *//
//*                                                                 *//
//*       NOTE           NOTE        NOTE         NOTE             *//
//* Please note that this job should only be run when the           *//
//* RACF subsystem address space has been taken down using the      *//
//* procedure that is documented in the RACF publications.          *//
//*       NOTE           NOTE        NOTE         NOTE             *//
//*                                                                 *//
//* Modify the JOB statement to fit your installation's             *//
//* requirements before executing it.                               *//
//*                                                                 *//
//* You will need to change the following:                          *//
//*                                                                 *//
//*      prefix      - To the PREFIX name you specified             *//
//*                    on the TARGET command for this node.         *//
//*                                                                 *//
//*      nodename    -  Is the name given to the RRSF node via      *//
//*                    the TARGET command that defined it.          *//
//*                                                                 *//
//*      sysname     - Is the CVTSNAME of the local system.         *//
//*                                                                 *//
//*      local-node  - Is the nodename associated with the          *//
//*                    local node.                                  *//
//*                                                                 *//
//*      remote-node - Is the nodename associated with the          *//
//*                    remote node.                                 *//
//*                                                                 *//
//*      local-lu    - Is the LU name associated with the           *//
//*                    local node or system.                        *//
//*                                                                 *//
//*      remote-lu   - Is the LU name associated with the           *//
//*                    remote node or system.                       *//
//*                                                                 *//
//*                                                                 *//
//*      NOTE: THE REMAINING KEYWORDS SHOULD NOT BE ALTERED.        *//
//*                                                                 *//
//*****************************************************************//
```

Figure 20 (Part 1 of 2). JCL to Rename the Workspace Data Sets

```
//RRSFALTR JOB 'JOB TO RENAME WORKSPACE DATA SETS',MSGLEVEL=1,1
//*
//* USE A JOBCAT OR STEPCAT WHERE NEEDED TO POINT TO THE CATALOG
//* THAT CONTAINS THE INFORMATION NEEDED FOR YOUR DATA SETS.
//*
//STEP1    EXEC  PGM=IDCAMS
//* THE WORKSPACE DATA SETS THAT REFER TO THE LOCAL SYSTEM SHOULD
//* BE CHANGED AS FOLLOWS:
//SYSPRINT DD    SYSOUT=*
//SYSIN    DD    *
    ALTER -
         prefix.local-node.local-node.INMSG -
         NEWNAME(prefix.sysname.INMSG)
    ALTER -
         prefix.local-node.local-node.INMSG.INDEX -
         NEWNAME(prefix.sysname.INMSG.INDEX)
    ALTER -
         prefix.local-node.local-node.INMSG.DATA  -
         NEWNAME(prefix.sysname.INMSG.DATA)
    ALTER -
         prefix.local-node.local-node.OUTMSG -
         NEWNAME(prefix.sysname.OUTMSG)
    ALTER -
         prefix.local-node.local-node.OUTMSG.INDEX -
         NEWNAME(prefix.sysname.OUTMSG.INDEX)
    ALTER -
         prefix.local-node.local-node.OUTMSG.DATA -
         NEWNAME(prefix.sysname.OUTMSG.DATA)
//STEP2    EXEC  PGM=IDCAMS
//* THE WORKSPACE DATA SETS THAT BACKUP THE RRSF TRANSACTIONS SENT TO
//* AND RECEIVED FROM OTHER SYSTEMS SHOULD BE CHANGED AS FOLLOWS:
//SYSPRINT DD    SYSOUT=*
//SYSIN    DD    *
    ALTER -
         prefix.local-node.remote-node.INMSG -
         NEWNAME(prefix.local-lu.remote-lu.INMSG)
    ALTER -
         prefix.local-node.remote-node.INMSG.INDEX -
         NEWNAME(prefix.local-lu.remote-lu.INMSG.INDEX)
    ALTER -
         prefix.local-node.remote-node.INMSG.DATA -
         NEWNAME(prefix.local-lu.remote-lu.INMSG.DATA)
    ALTER -
         prefix.local-node.remote-node.OUTMSG -
         NEWNAME(prefix.local-lu.remote-lu.OUTMSG)
    ALTER -
         prefix.local-node.remote-node.OUTMSG.INDEX -
         NEWNAME(prefix.local-lu.remote-lu.OUTMSG.INDEX)
    ALTER -
         prefix.local-node.remote-node.OUTMSG.DATA -
         NEWNAME(prefix.local-lu.remote-lu.OUTMSG.DATA)
/*
```

Figure 20 (Part 2 of 2). JCL to Rename the Workspace Data Sets

RACF Storage Considerations

This section discusses storage considerations for RACF.

Virtual Storage

Figure 21 estimates RACF virtual storage usage, for planning purposes.

Figure 21 (Page 1 of 2). RACF Estimated Storage Usage

Storage Subpool	Usage	How to Estimate Size
FLPA	RACF service routines, if IMS or CICS is using RACF for authorization checking	47 000
	RACROUTE REQUEST=FASTAUTH and ICHRTX00 exits	Measure using AMBLIST
PLPA	RACF installation exits that are AMODE(24) or AMODE(ANY)	Measure using AMBLIST
	RACF RMODE(24) code	750
	RACF service routines, if IMS or CICS is not using RACF for authorization checking, unless explicitly removed from SYS1.LPALIB and placed elsewhere for use in FLPA	47 000
	RACROUTE REQUEST=FASTAUTH and ICHRTX00 exits	Measure using AMBLIST
	RACF range table	4 + (number_of_ranges × 45)
EPLPA	RACF installation exits that are AMODE(31)	Measure using AMBLIST
	RACF above-the-line resident modules	875 000
SQA	RACF communications vector table and extension	2800
	Class descriptor table (CNST) and RACF router table	7500 + 58 × number_of_customer_defined_classes
ESQA	RACF data sharing control area	300 (when enabled for sysplex communication)
	Class descriptor table (CNSX)	(number_of_IBM-defined_classes × 28) + (number_of_IBM-defined_entries_in_router_table × 30) + (number_of_customer_defined_classes × 58) + 26 For Security Server (RACF) Release 2, there are 43 IBM-defined classes and 165 IBM-defined entries in the router table, so the size of the CNSX is 6180 + (number_of_customer_defined_classes × 58). If you install a PTF that adds entries, you will need to recalculate this number.
LSQA	ACEE and related storage **Notes:** 1. Applications can place this storage in a different subpool. 2. Applications can create multiple ACEEs in this and other storage subpools.	400 + installation_data_length + terminal_installation_data_length + application_installation_data + (52 for every 78 temporary datasets, rounded up to the next multiple of 52) If the address space has been dubbed an OpenEdition process, then add: 52 + (number_of_connected_groups_with_GIDs × 4) Add 112 bytes if the user has CLAUTH for a class with a POSIT value over 127.

Formula for average_profile_size:

average_profile_size = 51 + average_installation_data + (average_number_of_access_entries × 9) + (average_number_of_categories × 2) + (average_number_of_conditional_access_entries × 17)

Figure 21 (Page 2 of 2). RACF Estimated Storage Usage

Storage Subpool	Usage	How to Estimate Size
ELSQA	Connect group table	64 + (48 × number_of_groups_connected)
	In-storage generic profiles	160 + number_of_generic_profiles × (14 + average_profile_size + average_profile_name_length)
	RACF storage tracking table	3500
	RACROUTE REQUEST=LIST profiles **Note:** Applications can place these profiles in a different storage subpool.	52 + (number_of_profiles_in_class × 16) + (number_of_resident_profiles × (10 + average_profile_size + (1.5 × class_max_profile_name_size))) for each class if GLOBAL=YES is not specified
CSA	RACF global access tables	3040 + (number_of_user_classes × 24) + 2 × (18 + number_of_entries × (6 + (1.5 × max_profile_name_size)))
	RACF database control structures (DCB, DEB, templates)	4600 + (number_of_BAM_blocks × 6) + (364 x number_of_RACF_primary_data_sets)
	RACF subsystem control blocks	3500
ECSA	RACF data set descriptor table and extension	168 + (896 × number_of_RACF_primary_data_sets)
	RACF ICB (non-shared DB)	4096 per RACF database if the database is not shared and is not on a device marked as shared, 0 otherwise
	RACF program control table	105 × average_profile_name_length
	RACF resident data blocks	For each primary RACF database: 3248 + (4136 × number_of_database_buffers) If using sysplex communication, for each backup database add: 3248 + (4136 × number_of_database_buffers × .2)
	Dynamic parse tables	30 000
	SETROPTS GENLIST profiles	52 + (number_of_profiles_in_class × 16) + (number_of_resident_profiles × (10 + average_profile_size + (1.5 × class_max_profile_name_size)))
User private Below 16MB	RACF transient storage	16 000 (minimum) while a RACF service is executing

Formula for average_profile_size:

average_profile_size = 51 + average_installation_data + (average_number_of_access_entries × 9) + (average_number_of_categories × 2) + (average_number_of_conditional_access_entries × 17)

Customer Additions to the CDT

Additional classes can be defined in the CDT during installation, or they can be customized later. See “Customer Additions to the CDT” on page 35 for further information on installation-defined CDT classes.

Templates for RACF on OS/390 Release 2

The RACF database must have templates at the Security Server (RACF) Release 2 level in order for RACF to function properly. If a Security Server (RACF) Release 2 system is sharing the database with a lower-level system (RACF 1.9, RACF 1.9.2, RACF 1.10, RACF 2.1, RACF 2.2, or Security Server (RACF) Release 1), the lower-level system is able to use the database with the Security Server (RACF) Release 2 templates. Use the IRRMIN00 utility to install the templates.

For more information, see *OS/390 Security Server (RACF) System Programmer's Guide* and the program directory shipped with the product.

Chapter 6. Customization Considerations

This chapter identifies customization considerations for RACF.

For additional information, see *OS/390 Security Server (RACF) System Programmer's Guide*.

Customer Additions to the CDT

Installations must verify that classes they have added to the class descriptor table (CDT) do not conflict with new classes shipped with RACF. If duplicate CDT entries are detected, the following error messages are issued at IPL time:

- For a duplicate router table entry, RACF issues this message and continues processing: `ICH527I RACF DETECTED AN ERROR IN THE INSTALLATION ROUTER TABLE, ENTRY class_name, ERROR CODE 1.`
- For a duplicate CDT entry, RACF issues this message and enters failsoft mode: `ICH511I RACF DETECTED AN ERROR IN THE INSTALLATION CLASS DESCRIPTOR TABLE, ENTRY class_name, ERROR CODE 7.`

If a conflict in class names occurs, you must delete the profiles in the installation-defined class with the conflicting name, delete the CDT entry for the class, add a CDT entry with a different name, and redefine the profiles.

Do not assemble the user-defined CDT (ICHRRCDE) on OS/390 Release 2 and attempt to use it on a system running RACF at a lower level than RACF 2.2.

Exit Processing

Installation-written exits might be affected by new function introduced in OS/390 Release 2 Security Server (RACF).

Effects of OS/390 OpenEdition DCE Support on ICHRCX01, ICHRCX02, and IRRSXT00

OS/390 OpenEdition DCE support can affect:

- The RACROUTE REQUEST=AUTH preprocessing and processing exits
- The IRRSXT00 installation exit

RACROUTE REQUEST=AUTH Preprocessing and Postprocessing Exits

RACF support for OS/390 OpenEdition DCE introduces new indicators in the ACEE. These indicators mark the ACEE as a *client ACEE*. Client ACEEs are created by OS/390 OpenEdition and RACF on behalf of multithreaded unauthorized application servers on OS/390. There are two types of client ACEE:

- Unauthenticated client ACEE

  When an unauthenticated client ACEE is used in an access control decision, two authorization checks occur.

- The first check uses the client ACEE. This is the ACEE that is associated with the current task. If the request is successful, the second check is performed.
- The second check uses the ACEE associated with the server. This is the same ACEE that is associated with the address space.

When each of these checks occurs, the RACF exits ICHRCX01 and ICHRCX02 are invoked.

- Authenticated client ACEE

  When an authenticated client ACEE is used in an access control decision, only this ACEE is used in the access control decision. Audit records recorded contain an additional relocate section indicating that this authorization request was processed using an ACEE created on behalf of an unauthorized application.

IRRSXT00 Installation Exit

IRRSXT00 is invoked by the SAF callable services router before and after RACF is called. If your system already uses the IRRSXT00 installation exit, you should review this exit to be sure the following are true for the R_dceinfo and R_dceruid callable services:

- IRRSXT00 is capable of executing in either problem or supervisor state.
- IRRSXT00 does not expect to receive control in a system storage protection key (0-7).

RACROUTE REQUEST=DEFINE Preprocessing Exit (ICHRDX01)

Processing of a RETPD value specified via the RACROUTE REQUEST=DEFINE preprocessing exit has changed. Formerly, a RETPD value specified in an ICHRDX01 exit was not recorded in the profile when a generic profile was being defined, unless RETPD was also specified via command. Now, a RETPD value specified in an ICHRDX01 exit is picked up. If you do not want the value to be picked up when creating a generic profile, you should modify your exit to set the RETPD value only when processing a tape profile.

Chapter 7. Administration Considerations

This chapter summarizes the changes to administration procedures that the security administrator should be aware of. For more information, see *OS/390 Security Server (RACF) Security Administrator's Guide*.

OS/390 OpenEdition DCE

The interoperation of RACF with OS/390 OpenEdition DCE enables DCE application servers on MVS to map a DCE user identity *(principal)* to a RACF user ID. The mapping of a DCE principal to a RACF user ID is known as *cross-linking*. The cross-linking information contained in the RACF database can be used by:

- OS/390 OpenEdition DCE, for determining which MVS users are eligible for OS/390 OpenEdition DCE single signon to DCE
- Application servers residing on OS/390, to determine the RACF user ID of clients. For more information on application servers and their use of identity cross-linking contained in RACF, see "OS/390 OpenEdition DCE Application Considerations" on page 39.

To support the *cross-linking* and *single signon to DCE* features, RACF provides:

- The DCE segment for the RACF user profile
- The DCEUUIDS general resource class

The DCE segment, defined to the RACF user profile, associates a DCE principal with the RACF user profile. See Figure 17 on page 20 for the contents of the DCE segment.

The DCEUUIDS general resource class contains the cross-linking information for each RACF/DCE user. Profiles defined to the RACF DCEUUIDS class associate a DCE principal with a RACF user ID on a particular system that is part of a DCE cell.

The security administrator must work with the DCE administrator to define RACF profiles to support the *cross-linking* and *single signon to DCE* features.

Cross-Linking Between RACF Users and DCE Principals

Profiles in the DCEUUIDS class establish a cross-link between a DCE principal UUID and a RACF user ID. Two OpenEdition DCE utilities administer DCE information in the RACF database and create the initial cross-link information between the RACF user profile and the DCE principal registry:

mvsimpt is a two-pass utility that creates DCE principal entries in the DCE registry for the set of RACF users chosen to be cross-linked, based on the output from the RACF database unload utility. The unloaded RACF database is sorted by the administrator according to RACF user IDs with a RACF DCE segment and filtered by the utility according to processed entries from previous mvsimpt and mvsexpt processing.

mvsexpt is a two-pass utility that populates a RACF database with information for a set of DCE principals. It creates and updates the RACF DCE segment for each DCE principal being cross-linked with the RACF

database. The mvsexpt utility takes a specified input file or the DCE registry for each principal specified and creates the RACF DCE segment and profiles in the RACF general resource class, DCEUUIDS.

For more information on these utilities, see *OpenEdition DCE Administration Guide*.

Although you can administer the DCEUUIDS profiles using the RACF RDEFINE and RALTER commands, it is *strongly recommended* that you use the OS/390 OpenEdition DCE utilities.

Attention

Changing the UUID or HOMEUUID fields in a user profile DCE segment via RACF commands (such as ADDUSER, ALTUSER, or DELUSER) does *not* update DCEUUIDS class profiles. It is strongly recommended that you use the OS/390 OpenEdition DCE utilities to maintain the DCE information contained within RACF.

The OS/390 OpenEdition DCE utilities maintain a file of users that have been processed. If you perform subsequent administration, and do not use the utilities, the processed entry file might not be accurate. Inaccuracies in this file can cause unpredictable results the next time the OpenEdition DCE utilities are used.

Activating the DCEUUIDS Class

Before OS/390 OpenEdition DCE can use profiles defined to the DCEUUIDS class, the security administrator must activate the class. To activate the DCEUUIDS class enter:

```
SETROPTS CLASSACT(DCEUUIDS)
```

Single Signon to DCE

RACF support for OS/390 OpenEdition DCE provides for a *single signon to DCE*. OS/390 OpenEdition DCE single signon signs an MVS user on to DCE automatically if that user has already been authenticated by RACF. To start single signon to DCE processing, the following conditions must be met:

- The security administrator has requested single signon to DCE processing for the user.
- The security administrator has defined the DCE encryption key.
- The user is not currently logged into DCE.
- The user invokes a DCE application.
- The user is defined as a DCE principal to the DCE registry.

Before OpenEdition DCE single signon support can be invoked for an MVS user, the MVS user must be enrolled for single signon to DCE. To enroll:

- RACF setup procedures for DCE interoperability must be completed.
- A DCE segment must be created for the MVS user in the RACF user profile. The user profile DCE segment must contain the user's DCE information.
- The AUTOLOGIN value in the user's DCE segment must be set to YES to invoke single signon processing. If the value is set to NO, single signon to DCE processing does not occur.

- The MVS user must have saved the current DCE password in the RACF DCE segment by invoking the DCE **storepw** command.

  Note: Users still need to maintain their passwords for RACF and OpenEdition DCE separately, and must use the DCE **storepw** to keep the DCE password that is stored in RACF current.

Single signon support is *not* intended to be used by application servers. Single signon support should be enabled only for end users. For more information on single signon restrictions see *OpenEdition DCE Administration Guide*.

Specifying the DCE Encryption Key

The RACF KEYSMSTR class is a general resource class that contains the DCE.PASSWORD.KEY profile. This profile holds the encryption key that is used for encrypting and decrypting a user's DCE password for use in OpenEdition DCE single signon support. The profile defined to the KEYSMSTR class contains a SSIGNON segment that holds either the masked or encrypted value for the key that is used to encrypt DCE passwords stored in the RACF database. Before an OS/390 user can save a DCE password in the RACF database or before the DCE single signon feature can be used, the security administrator must define the profile to the KEYSMSTR class that defines the encryption key, and activate the KEYSMSTR class.

If a cryptographic product is present on the system, the security administrator can specify the KEYENCRYPTED sub-operand on the SSIGNON operand of the RDEFINE or RALTER command. If the KEYENCRYPTED sub-operand is specified, the cryptographic product must be active when the security administrator defines the profile to the KEYSMSTR class.

OS/390 OpenEdition DCE Application Considerations

OS/390 OpenEdition has two fundamental types of application servers:

- Multithreaded applications
- Single threaded applications

A *multithreaded* application has multiple sequential flows of control. In this type of application, more than one unit of work at a time is processed by the server application.

A *single threaded* application has one sequential flow of control. In this type of application, one unit of work is processed at a time by the application server.

OS/390 OpenEdition provides an S/390 assembler callable service and support through the C runtime library. This support enables *unauthorized* multithreaded applications to create and delete a RACF ACEE in a fashion that is mediated and controlled by the MVS OpenEdition kernel and RACF. The term *unauthorized* refers to applications that are not APF-authorized and do not run in supervisor state or in a system storage protection key.

The **pthread_security_np** service enables multithreaded applications to customize the security environment of a thread, meaning that the thread can execute under a different RACF identity than the server. The use of the **pthread_security_np** callable s000000000 the C runtime library **pthread_security_np()** API requires administration by the security administrator. Administrative considerations of the MVS OpenEdition **pthread_security_np** callable service are discussed in *OS/390*

OpenEdition Planning, and in *OS/390 OpenEdition Programming: Assembler Callable Services Reference*. The C language support for the **pthread_security_np()** function is discussed in *OS/390 R2 C/C++ Run-Time Library Reference*.

Threads and Security

An application that uses the **pthread_security_np** service can customize the RACF identity of a thread. Consider a DCE application server on OS/390, which accepts requests through DCE remote procedure calls (RPC). This server initiates a thread that processes the client's request. If the server customizes the thread initiated for the client with the client's RACF identity, any resource access decisions to MVS RACF-protected resources are made using the client's RACF identity and authorizations.

The security administrator has the option of enforcing both the application server's RACF identity *and* the RACF identity of the client to be used in resource access control decisions on OS/390.

The use of the **pthread_security_np** service is partially protected through a RACF FACILITY class profile BPX.SERVER.

- Application servers that have UPDATE access to this profile can act as a surrogate of the client.[2] This means that only the client's RACF identity and authorizations are used in resource access decisions processed by RACF.
- If the application servers are permitted with READ access to the RACF FACILITY class profile BPX.SERVER, two identities are used in local access control decisions on OS/390:
  - The RACF identity of the client
  - The RACF identity of the server

  RACF authorization processing enforces the requirement that *both* the MVS user ID associated with the client and the MVS user ID associated with the server are authorized to the resource being checked. This capability enables an installation to control:
  - Which user IDs the server can act on behalf of
  - What resources the server can access when acting on behalf of one of its clients

This additional security checking might require additional RACF administration to authorize the server to the RACF resource profiles that the server accesses on behalf of its clients.

Single threaded applications cannot use the **pthread_security_np** service to manage a RACF ACEE.

---

[2] There is an additional security check in which a RACF SURROGAT class profile must authorize the server to act as a surrogate for the client. For more information see *OS/390 OpenEdition Planning*.

Changes to RACF Authorization Processing

Extensions have been introduced to RACF's processing of authorization requests in which *both* the RACF identity of the server *and* the RACF identity of a client of the server application are used in a resource access decision.

RACF support for OpenEdition DCE introduces new indicators in the ACEE. These indicators mark the ACEE as a *client ACEE*. Client ACEEs are created by OS/390 OpenEdition and RACF on behalf of multithreaded unauthorized application servers on OS/390.

Client ACEEs can only be created through the OS/390 OpenEdition **pthread_security_np** callable service or **pthread_security_np()** C language function call.

There are two types of client ACEEs:

- Unauthenticated client ACEE

  When an unauthenticated client ACEE is used in an access control decision, two authorization checks occur.

  – The first check uses the client ACEE. This is the ACEE that is associated with the current task. If the request is successful, the second check is performed.

  – The second check uses the ACEE associated with the server. This is the same ACEE that is associated with the application server's address space.

  The automatic checking of both the client's identity and the server's identity is performed for RACF resources defined to RACF via profiles and for OS/390 OpenEdition resources, such as hierarchical file system files (HFS), whose access is governed by POSIX permission bits.
- Authenticated client ACEE

  When an authenticated client ACEE is used in an access control decision, only this ACEE is used in the access control decision. Audit records contain an additional relocate section, indicating that this authorization request was processed using an ACEE which was created on behalf of an unauthorized application.

  An authenticated client ACEE is created when the client of the server application has supplied its RACF password (or RACF PassTicket) to the application server. The application server specifies the client's RACF password (or RACF PassTicket) on the **pthread_security_np** OS/390 OpenEdition callable service or on the C language **pthread_security_np()** function call.

Restrictions

The security administrator must be aware of the restrictions of the RACF client ACEE support, in which both the application server's RACF identity and the client's RACF identity are used in resolving access decisions.

- RACROUTE REQUEST=FASTAUTH processing has not been enhanced to automatically check both the server and client RACF identities.

  Ideally, application servers on OS/390 do not have to run APF-authorized, or in supervisor state or in a system storage protection key. Unauthorized application servers on OS/390 are therefore unable to use the RACROUTE REQUEST=LIST instruction to build in-storage profiles for RACF-defined

resources. Profiles must reside in storage before RACROUTE REQUEST=FASTAUTH can be used to verify a user's access to a resource.

- The client/server relationship is not propagated from the application server.

If the security administrator implements access control to resources that use *both* the server's RACF identity and the client's RACF identity in an access control decision, application servers that the security administrator does not trust should be treated as *end points* on OS/390. These servers should *not* be allowed to submit batch jobs or use the services of other servers that run exclusively under the identity of the client. This is because the relationship of the client and server identity pair is not propagated to other applications or servers. The security administrator must enforce this through administrative procedures by ensuring that applications servers that do not meet this criteria are *not* authorized to the profile BPX.SERVER in the RACF FACILITY class. By denying the untrusted servers authorization to BPX.SERVER, the security administrator ensures that all work done by the server, including job submission and the use of other servers, occurs using the server's identity.

Controlling the R_dceruid Callable Service

The security administrator must define the IRR.RDCERUID profile in the FACILITY class to control the use of the SAF R_dceruid callable service. This callable service maps the DCE UUID to the RACF user ID.

Check your installation for programs that use:

- the SAF R_dceruid callable service

or services that call it, such as:

- the OS/390 OpenEdition **convert_id_np** callable service
- the C library function **__convert_id_np()** function call

Users or servers using programs that use these services must have READ access or higher to the profile that protects IRR.RDCERUID in the FACILITY class.

Enhancements to the Remove ID Utility

The RACF remove ID utility, IRRRID00, has been enhanced to search profiles defined to the DCEUUIDS class when removing a user ID. The utility generates output consisting of commands that remove DCEUUIDS class profiles in which the APPLDATA field contains the user ID being removed.

The RACF security administrator should contact the DCE administrator when removing a user ID which has been cross-linked with a DCE principal, to determine if the DCE principal should be deleted from the cell.

SOMobjects for MVS

The security administrator must permit the users who are allowed to use specific SOM servers and are allowed to use specific methods within classes to profiles within the new RACF CBIND and SOMDOBJS classes. In addition, the security administrator must define which servers are known to the SOM daemon, by defining profiles within the new RACF SERVER class.

SystemView for MVS

Before an installation can use SystemView for MVS, the security administrator must:

- Create profiles in the SYSMVIEW class for SystemView for MVS applications. The profiles define logon script and parameter information for the applications.
- Authorize SystemView for MVS users to access the defined applications via the SystemView for MVS Launch window.

For information about SystemView for MVS and the Launch window, see *SystemView for MVS Up and Running!*.

Chapter 8. Auditing Considerations

This section summarizes the changes to auditing procedures for the RACF:

- SMF records
- Report writer utility
- SMF data unload utility

The auditor must decide on appropriate global auditing options for the new classes and on which auditing reports are to be produced. See *OS/390 Security Server (RACF) Auditor's Guide* and *OS/390 Security Server (RACF) Macros and Interfaces* for more information.

SMF Records

Figure 22 summarizes the new event codes for SMF records created by RACF for OS/390 Release 2. The new event code is a general-use programming interface (GUPI).

Figure 22. New Event Codes

Event Code	Description	Support
65	Audits the passing of access rights from one process to another.	OS/390 OpenEdition

Figure 23 summarizes changes to SMF records created by RACF for OS/390 Release 2. These changes are general-use programming interfaces (GUPI).

Figure 23 (Page 1 of 2). Changes to SMF Records

Record Type	Record Field	Description of Change	Support
80	SMF80EVT	Event code 57 is used to audit two new OpenEdition services: a new console communications service (CCS) and a new workload manager (WLM) service. Two new audit function codes, 99 and 100, cause event 57 records to be generated. Creation of the audit records is controlled by the existing PROCESS class. Event code 65 is used to audit the passing of access rights from one process to another. Three new audit function codes, 95, 96, and 97, cause event 65 records to be generated. Creation of the audit records is controlled by the existing PROCACT class.	OS/390 OpenEdition
80	Relocate 64	For event code 2, this SMF record contains a link value to connect client and server audit records.	OS/390 OpenEdition DCE

Figure 23 (Page 2 of 2). Changes to SMF Records

Record Type	Record Field	Description of Change	Support
80	Relocate 65	For event code 2, this SMF record contains flags indicating the ACEE type: • Unauthenticated client • Authenticated client • Server	OS/390 OpenEdition DCE
80	Relocate 315	For event codes 28, 29, 30, 31, 32, 33, 34, 41, 44, 47, 48, 54, 55, 56, 57, 63, and 64, this SMF record contains a link value to connect client and server audit records.	OS/390 OpenEdition DCE
80	Relocate 316	For event codes 28, 29, 30, 31, 32, 33, 34, 41, 44, 47, 48, 54, 55, 56, 57, 63, and 64, this SMF record contains flags indicating the ACEE type: • Unauthenticated client • Authenticated client • Server	OS/390 OpenEdition DCE

For more information on SMF records, see *OS/390 Security Server (RACF) Macros and Interfaces*.

Auditing New OS/390 OpenEdition MVS Services

RACF provides two new audit function codes (99 and 100) to audit two new OS/390 OpenEdition MVS services: a new console communications service (CCS) and a new workload manager (WLM) service. Creation of the audit records is controlled by the existing PROCESS class. Customers that are not already auditing the PROCESS class must issue `SETROPTS AUDIT(PROCACT)` to obtain the new SMF records, where *option* is ALWAYS, NEVER, SUCCESSES, FAILURES, or DEFAULT. Customers that are already auditing the PROCESS class automatically receive the new SMF records. These customers might see an increase in the number of SMF records that RACF writes during OpenEdition processing.

RACF also provides three new audit function codes (95, 96, and 97) to audit the passing of access rights from one process to another. Creation of the audit records is controlled by the existing PROCACT class. Customers that are not already auditing the PROCACT class must issue `SETROPTS LOGOPTIONS(`*`option`*`(PROCACT))` to obtain the new SMF records, where *option* is ALWAYS, NEVER, SUCCESSES, FAILURES, or DEFAULT. Customers that are already auditing the PROCACT class automatically receive the new SMF records. These customers might see an increase in the number of SMF records that RACF writes during OpenEdition processing.

Auditing OS/390 OpenEdition DCE Support

RACF provides one new audit function code (94) to audit OS/390 OpenEdition DCE support.

Auditing SystemView for MVS Support

Depending on the auditing options selecting when using the RACF SMF data unload utility (IRRADU00), customers might see SMF records returned for the new SYSMVIEW class and type 44 relocate sections for the new SVFMR segment.

Report Writer

The RACF report writer has not been enhanced since RACF 1.9.2, and it will not be enhanced in the future. It is able to process the SMF records created for RACF on OS/390 Release 2, but it is not able to report on most new RACF function.

Certain RACF enhancements automatically handled by the report writer are still reported; for example:

- SETROPTS options that affect new RACF classes
- Access successes or failures for resources in new RACF classes

Installations using the RACF report writer must change to another reporting package to obtain full reports from RACF SMF records. However, because the SMF data unload utility (IRRADU00) does not unload the text of the RVARY or SETROPTS commands, installations that want this information from the SMF data must use the RACF report writer.

SMF Data Unload Utility

The SMF data unload utility (IRRADU00) is updated to support all the SMF record changes for RACF on OS/390 Release 2. These changes are summarized in “SMF Records” on page 45.

The SMF data unload utility creates a new access rights extension record when access rights are passed, to support OS/390 OpenEdition.

Chapter 9. Operational Considerations

This section summarizes the changes to operating procedures for RACF for OS/390 Release 2.

Enhancements to the RESTART Command

The RESTART command has been enhanced. The new SYSNAME keyword allows an operator to restart connections to systems on a multisystem node. See *OS/390 Security Server (RACF) Command Language Reference* for more information.

Enabling and Disabling RACF

The Security Server (RACF) for OS/390 Release 2 supports the OS/390 enable and disable functions. Entries in the IFAPRD*xx* parmlib member specify which features are enabled and disabled.

If RACF is not enabled on your system when you IPL, RACF initialization does not complete, message IFA104I is issued, and RACF does not provide security for the system. If you plan to use RACF, make sure that an entry exists in IFAPRD*xx* to enable RACF before you IPL. To see what the entry should look like, see "Enabling RACF" on page 27.

To disable RACF, update the IFAPRD*xx* member for RACF, setting the STATE field to `DISABLED`, and re-IPL. For more information, see *OS/390 Security Server (RACF) System Programmer's Guide* or *OS/390 MVS Product Management*.

Chapter 10. Application Development Considerations

Application development is the process of planning, designing, and coding application programs that invoke RACF functions. This section highlights new support that might affect application development procedures:

- Year 2000 support
- OS/390 OpenEdition DCE Application Servers
- Changes to the class descriptor table
- Programming interfaces

Year 2000 Support

RACF provides a date conversion routine, IRRDCR00. Programs can call IRRDCR00 to convert a RACF 3-byte packed decimal date in the form *yyddd*F into a 4-byte packed decimal date in the form *ccyyddd*F, where *cc* is 00 for dates in the range 1971-1999 and 01 for dates in the range 2000-2070. The routine returns a date in the form:

00*yyddd*F if *yy* is 71 or higher
01*yyddd*F if *yy* is less than 71

For more information on IRRDCR00, see *OS/390 Security Server (RACF) Macros and Interfaces*.

OS/390 OpenEdition DCE Application Servers

OS/390 OpenEdition has two fundamental types of application servers:

- Multithreaded applications
- Single threaded applications

A *multithreaded* application has multiple sequential flows of control. In a multithreaded application, more than one unit of work at a time is processed by the server application.

A *single threaded* application has one sequential flow of control. In a single threaded application, one unit of work is processed at a time by the application server.

OS/390 OpenEdition provides an S/390 assembler callable service, the pthread_security_np service, and support through the C run time library. This support enables *unauthorized* (the term *unauthorized* refers to applications that are not APF-authorized and do not run in supervisor state or in a system storage protection key) multithreaded applications to create and delete a RACF ACEE, in a fashion that is mediated and controlled by the MVS OpenEdition kernel and RACF.

The pthread_security_np service enables multithreaded applications to customize the security environment of a thread, meaning that the thread can execute under a different RACF identity than the server. If the server customizes the thread initiated for the client with the client's RACF identity, any resource access decisions to MVS RACF-protected resources are made using the client's RACF identity and authorizations.

The security administrator has the option of enforcing the use of both the application server's RACF identity *and* the RACF identity of the client in resource access control decisions.

RACF support for OS/390 OpenEdition DCE introduces new indicators in the ACEE. These indicators mark the ACEE as a *client ACEE*. Client ACEEs are created by OS/390 OpenEdition and RACF on behalf of multithreaded unauthorized application servers on OS/390. Client ACEEs can only be created through the OS/390 OpenEdition **pthread_security_np** callable service or **pthread_security_np()** C language function call.

There are two types of client ACEEs:

- Unauthenticated client ACEE

  When an unauthenticated client ACEE is used in an access control decision, two authorization checks occur.

  – The first check uses the client ACEE. This is the ACEE that is associated with the current task. If the request is successful, the second check is performed.

  – The second check uses the ACEE associated with the server. This is the same ACEE that is associated with the application server's address space.

  The automatic checking of both the client's identity and the server's identity is performed for RACF resources defined to RACF via profiles and for OS/390 OpenEdition resources, such as hierarchical file system files (HFS), whose access is governed by POSIX permission bits.
- Authenticated client ACEE

  When an authenticated client ACEE is used in an access control decision, only this ACEE is used in the access control decision.

  An authenticated client ACEE is created when the client of the server application has supplied its RACF password (or RACF PassTicket) to the application server. The application server specifies the client's RACF password (or RACF PassTicket) on the **pthread_security_np** OS/390 OpenEdition callable service or on the C language **pthread_security_np()** function call. Possession of the client's RACF password (or RACF PassTicket) indicates that the client trusts the server to act on the client's behalf.

New Application Services and Security

Through OS/390 OpenEdition MVS, the C run time library, and RACF, two new services are available that enable application servers on OS/390 to:

- Map a DCE identity to a RACF user ID, or map a RACF user ID to a DCE identity
- Invoke RACF authorization services

The service convert_id_np (BPX1CID) is the OS/390 OpenEdition MVS callable service that converts a DCE principal's UUID pair (cell UUID and principal UUID) to the RACF user ID that has been cross linked with the UUID pair. This service also accepts a RACF user ID and returns the corresponding DCE UUIDs. This OS/390 OpenEdition service is also supported through the C runtime library via the __convert_id_np() function call. The use of these mapping functions is RACF-protected.

For more information on the convert_id_np (BPX1CID) callable service, see *OS/390 OpenEdition Programming: Assembler Callable Services Reference*. The C language support for the __convert_id_np() is discussed in *OS/390 R2 C/C++ Run-Time Library Reference*

New Application Authorization Service

A DCE application server on OS/390 can use DCE security services for access control to resources that are owned by the application server. As an alternative, the application developer can use RACF for access control for the set of resources that are managed by the application server.

Consider that application servers that use DCE services exclusively on OS/390 are the most portable to platforms that support DCE. If portability is not a primary concern and the application developer wishes to centralize access control list information in RACF, the application developer can consider using the auth_check_resource_np service.

Through OS/390 OpenEdition MVS, a new a callable service auth_check_resource_np (BPX1ACK) enables application servers to invoke RACF authorization services. This callable service is also supported by the C runtime library through the __check_resource_auth_np() function call. This service allows application servers to perform authorization requests for resources that are defined to RACF general resource classes.

For more information on the auth_check_resource_np callable service, see *OS/390 OpenEdition Programming: Assembler Callable Services Reference*.

Changes to the Class Descriptor Table

The maximum length of profile names has changed for the following classes:

- INFOMAN
- GINFOMAN
- JCICSJCT
- KCICSJCT

This change might require changes to customer code which uses these classes on:

- RACROUTE REQUEST=FASTAUTH
- RACROUTE REQUEST=AUTH, DEFINE, or EXTRACT, if the ENTITY keyword is used instead of ENTITYX

IBM products should not need changes, because their usage of these fields is compatible with this change.

Programming Interfaces

For a summary of changes to the programming interfaces for RACF for OS/390 Release 2, see:

- "Class Descriptor Table (CDT)" on page 13
- "Data Areas" on page 16
- "Exits" on page 16

- “Macros” on page 17
- “Templates” on page 20
- “Utilities” on page 21
- “Routines” on page 19

Chapter 11. General User Considerations

RACF general users use RACF to:

- Log on to the system
- Access resources on the system
- Protect their own resources and any group resources to which they have administrative authority

This chapter highlights new support that might affect general user procedures.

OS/390 OpenEdition DCE

If an installation has implemented single signon to DCE, an MVS user can be logged on to DCE automatically without entering a DCE password, if that user has already been authenticated by RACF. However, the user must continue to separately maintain passwords for DCE and RACF. Whenever a user changes the DCE password that is known to the DCE registry, the user must use the DCE storepw command to save the new DCE password in the RACF database. See *OpenEdition DCE Command Reference* for information on the storepw command.

Chapter 12. NJE Considerations

Several APARs shipped on OS/390 Release 2 Security Server (RACF) have implications for NJE.

APAR OW14451

OS/390 Release 2 Security Server (RACF) includes a PTF that provides functions that change the way inbound NJE jobs and NJE sysout are handled by RACF. If your installation uses NJE and RACF nodes profiles it is imperative that you read and understand this chapter before installing the new RACF release. This information includes a brief overview of NJE security before and after application of this release and the actions required to assure that the PTF has no unexpected consequences on your system. It also includes information on how you can use the enhanced function introduced by this PTF to further implement security for NJE on your system.

Note: APAR OW08457 shipped on RACF releases prior to RACF 2.2. The code that shipped for OW08457 was in the RACF 2.2 base program (the GA version) and OS/390 Release 1 Security Server (RACF). OW14451 fixes some problems introduced by OW08457 that are in the RACF 2.2 base and OS/390 Release 1 Security Server (RACF). The phrase “prior to OW08457” means “prior to RACF 2.2 and prior to OS/390 Release 1 Security Server (RACF).” In any case, OS/390 Release 2 Security Server (RACF) users should be aware of the possible implications of the changes OW08457 and OW14451 have on NJE processing.

Before Applying the PTF for APAR OW08457

Prior to the application of OW08457, RACF did not perform any security translation or propagation for groups associated with NJE jobs or SYSOUT. RACF uses profiles of the form NODEID.USER%.* ADDMEM(USERID) with a UACC or read or higher to translate USERIDs from the submitting userid to an execution USERID on the receiving system. This type of translation was not available for submitting groups. The execution group became the default group of the translated USERID.

After Applying the PTF for APAR OW08457

This PTF enables group translation and propagation for NJE jobs and SYSOUT. With this fix applied the submitting group is propagated to become the execution group for jobs and the owning group for SYSOUT in the absence of any applicable NODEID.GROUP%.GROUPID profiles. This service introduces the ability to translate groups with NODEID.GROUP%.GROUPID profiles by using an ADDMEM with a UACC of READ or higher. An ADDMEM of &DFLTGRP will cause the USERIDs default group to be used as the execution or owning group. A UACC of NONE on the GROUP% profile will work as it always has. Because NODES profiles only affect inbound NJE work, no profile changes need to be made for outbound NJE work.

Actions Required

With OW08457 and OW14451, group propagation and group translation has been fixed for NODES profiles, both for batch jobs and for SYSOUT. This change can significantly alter the external results of your NJE environment and your installation must decide what changes will best suit your needs.

Case 1: Nodes defined to &RACLNDE.

For nodes defined to the RACFVARS variable &RACLNDE, there is no change (group propagation still does not occur, and group translation was never relevant). It was determined that fixing group propagation for this case would cause too much disruption, so it was left unchanged. Remember that if a node is defined to &RACLNDE, no NODES profile lookup will take place.

Case 2: Getting NODES externals to work as they did prior to OW08457 and OW14451

Your installation might decide to continue to base NJE security primarily on the user ID, and let the resulting job or SYSOUT take that user ID's default-group for purposes of verification. This was the case prior to these APARs. These are the steps suggested for achieving the same effect with the revised externals:

Note: The changes listed below in steps 1 and 2 must be made on all nodes where you want processing to work as it did prior to OW08457 and OW14451.

Step 1:

Delete all GROUPJ and GROUPS NODES profiles that have a UACC value greater than or equal to READ. These profiles were previously irrelevant but now could result in failing jobs or unowned SYSOUT. Note that GROUPJ and GROUPS NODES profiles with a UACC value of NONE already worked and still work as documented.

Step 2:

Create a NODES profile of the format nodeid.GROUP%.* UACC(READ) ADDMEM(&DFLTGRP) for each node for which you expect inbound work. If no more-specific NODES profiles exist than nodeid.GROUP%.* that would protect inbound work(e.g. nodeid.*.*), the profile *.GROUP%.* UACC(READ) ADDMEM(&DFLTGRP) can be created instead of the individual nodeid.GROUP%.* profiles. After the NODES profiles are created, do any necessary refresh of in-storage profiles. The new profile(s) cause RACF to use the default group for NJE verification after the user ID has been propagated and possibly translated. Note that without step 1 above, there could be more specific GROUPJ and "GROUPS" profiles so that the &DFLTGRP wouldn't be used consistently, resulting in problems described above.

Case 3: Making use of group propagation in NJE security

Because group propagation and group translation were not functional until now, RACF recommends the following steps for making the transition to this function.

Step 1:

List all GROUPJ and GROUPS NODES profiles that have a UACC value greater than or equal to READ, recording the profile names and all keywords necessary to add them back later. Then delete them. These profiles were previously irrelevant but now could result in failing jobs or unowned SYSOUT. Note that GROUPJ and GROUPS NODES profiles with a UACC value of NONE already worked and still work as documented.

Step 2:

Create the NODES profile *.GROUP%.* with UACC(READ) and ADDMEM(&DFLTGRP), then do any necessary refresh of in-storage profiles. This profile causes RACF to use the default group for NJE verification, after the user ID has been propagated and possibly translated. This profile acts as a catch-all until all other GROUP NODES profiles have been verified.

Step 3:

Add more specific GROUP NODES profiles. Perhaps you are adding GROUP NODES profiles for the first time; see *OS/390 Security Server (RACF) Security Administrator's Guide* for their intended uses and externals. Take note of any batch job failures or SYSOUT owners assigned by SYSOUT FAILSAFE processing (SYSOUT message IRR808I will be displayed). Correct any problems in your profiles to accurately reflect corresponding users and groups on the different NJE nodes.

Step 4:

When your installation is confident that the GROUP profiles are set up correctly, change the one from step 2 to a UACC(NONE) with no ADDMEM. This generic profile now fails jobs or disowns SYSOUT when a more specific profile is not found.

APAR OW15408

If you are using NODES class profiles of the form *nodeid*.RUSER.*nodeid* to allow JOBs to enter a node, you can remove those RUSER nodes profiles. This form of NODES profile has been used as a problem bypass by users, to allow the copy of a second NJE Job into the JES internal reader using two /*XEQs.

Chapter 13. Scenarios

This chapter contains scenarios that might help you in planning your migration to Security Server (RACF) Release 2.

Migrating an Existing RRSF Network to Use Multisystem Nodes

If an existing RRSF network contains single-system RRSF nodes that share a RACF database, you can reconfigure the single-system RRSF nodes to a multisystem RRSF node. When you do this, the system that is the receiver in the existing RRSF network for the single-system RRSF nodes sharing a RACF database must be the main system for the multisystem node. If you want another system to be the main system, configure the receiver as the main system and then reconfigure the network with a new main system.

Figure 24 shows an RRSF network that does not have multisystem node support installed. MIAMI1, MIAMI2, and ORLANDO are RRSF nodes. MIAMI1 and MIAMI2 share a RACF database, and ORLANDO uses profiles in the RRSFDATA class to ensure that database updates are sent to only MIAMI1, the receiver.

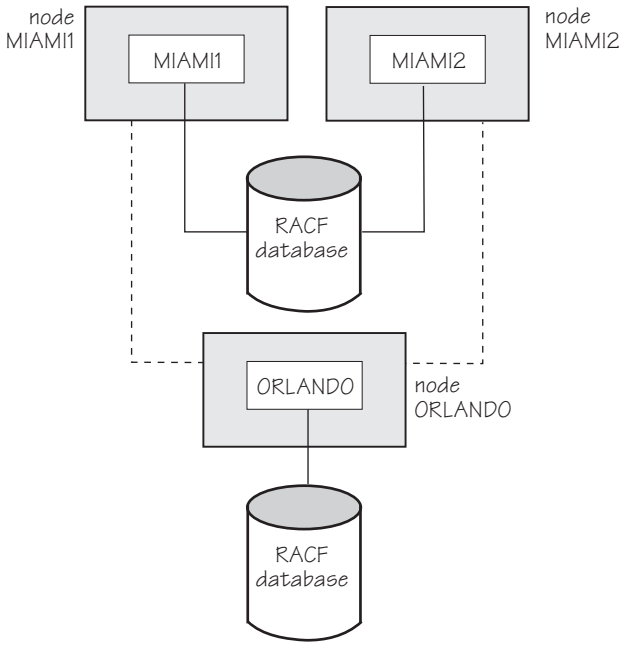


Figure 24. An RRSF Network Where Two Single System Nodes Share a RACF Database

This scenario illustrates how to migrate the RRSF network shown in Figure 24 to one implementing a multisystem node, after multisystem node support has been installed on MIAMI1, MIAMI2, and ORLANDO. Assume that the CVTSNAME for MIAMI1 is SYSTEM1, and the CVTSNAME for MIAMI2 is SYSTEM2.

On MIAMI1:

1. To ensure that RACF activity is stopped, take down TSO/E and JES. This should drain all RACF work from the system.

2. Issue TARGET DORMANT commands from the operator's console to make all RRSF conversations dormant:

   ```
   prefixTARGET NODE(MIAMI1) DORMANT
   prefixTARGET NODE(ORLANDO) DORMANT
   ```

3. Issue a TARGET command from the operator's console to make MIAMI1 the main system on the new multisystem node MIAMI1. The old node name is used for the new multisystem node because the existing RRSFDATA profiles on node ORLANDO already use this node name for all automatic command direction, automatic password direction, and RACLINK PWSYNC updates.

   ```
   prefixTARGET NODE(MIAMI1) SYSNAME(SYSTEM1) LOCAL MAIN OPERATIVE
   ```

   Update the corresponding command in the RACF parameter library, adding the MAIN and SYSNAME keywords, so that the updated command will be executed if the address space is recycled or the system is re-IPLed.

4. Issue a TARGET command from the operator's console to make MIAMI2 a non-main system on the new multisystem node MIAMI1.

   ```
   prefixTARGET NODE(MIAMI2) SYSNAME(SYSTEM2) LOCAL OPERATIVE
   ```

   Add the corresponding command to the RACF parameter library, adding SYSNAME keyword, so that the command will be executed if the address space is recycled or the system is re-IPLed.

On MIAMI2:

1. To ensure that RACF activity is stopped, take down TSO/E and JES. This action prevents MIAMI2 from updating the RACF database without sending the updates to ORLANDO's RACF database.

2. Issue TARGET DORMANT commands from the operator's console to make all RRSF connections dormant:

   ```
   prefixTARGET NODE(MIAMI2) DORMANT
   prefixTARGET NODE(ORLANDO) DORMANT
   ```

3. Issue TARGET DELETE commands from the operator's console to delete all RRSF connections:

   ```
   prefixTARGET NODE(ORLANDO) DELETE
   prefixTARGET NODE(MIAMI2) DELETE
   ```

   Update the RACF parameter library to delete the existing TARGET commands for RRSF connections.

   Another way you can do this step is to first make the updates to the RACF parameter library, then stop and restart the RACF address space:

   ```
   prefixSTOP
   START subsystem-name,SUB=MSTR
   ```

4. Issue a TARGET command from the operator's console to define MIAMI2 as a member system of the new multisystem node MIAMI1:

   ```
   prefixTARGET NODE(MIAMI1) SYSNAME(SYSTEM2) LOCAL OPERATIVE
          PREFIX(...) PROTOCOL(...) WORKSPACE(...)
   ```

   The system that was originally single-system RRSF node MIAMI2 is now system SYSTEM2 of multisystem node MIAMI1. Remember that this system name, SYSTEM2, must match the CVTSNAME for the system. Also add this command to the RACF parameter library for SYSTEM2.

5. Issue a TARGET command from the operator's console to define system SYSTEM1 as the MAIN system for the multisystem node. (Issuing this command allows you to reconfigure the node to make SYSTEM2 the main system at some future time.)

   ```
   prefixTARGET NODE(MIAMI1) SYSNAME(SYSTEM1) LOCAL MAIN OPERATIVE
          PREFIX(...) PROTOCOL(...) WORKSPACE(...)
   ```

   Add this command to the RACF parameter library for SYSTEM2.

On ORLANDO:

1. If MIAMI2 is the chosen destination of any autodirected output or notifications, change this destination to be node MIAMI1. For example:

   ```
   SET AUTODIRECT(NOTIFY(FAILURES(MIAMI1.ADMIN))
                  OUTPUT(FAILURES(MIAMI1.ADMIN)))
   ```

   All autodirected output and notifications are sent to the main system of a multisystem node.

2. Issue a TARGET DORMANT command from the operator's console to make the connection with MIAMI2 dormant:

   ```
   prefixTARGET NODE(MIAMI2) DORMANT
   ```

3. Ensure that the INMSG and OUTMSG workspace data sets for node MIAMI2 are empty. Automatic command direction and automatic password direction should have been directed to MIAMI1. But if the workspace data sets are not empty, use the RACF VSAM file browser utility, IRRBRW00, to record any remaining command requests. (See *OS/390 Security Server (RACF) Diagnosis Guide* and the RACJCL member of SYS1.SAMPLIB for information on IRRBRW00.)

   Note: Rerun the remaining commands after you complete step 5.

4. Issue a TARGET DELETE command from the operator's console to delete the RRSF connections with MIAMI2:

   ```
   prefixTARGET NODE(MIAMI2) DELETE
   ```

   Update the RACF parameter library to delete the existing TARGET commands for RRSF connections.

   Another way you can do this step is to first make the updates to the RACF parameter library, then stop and restart the RACF address space:

   ```
   prefixSTOP
   START subsystem-name,SUB=MSTR
   ```

5. Issue TARGET commands from the operator's console for the new multisystem node, MIAMI1:

   ```
   prefixTARGET NODE(MIAMI1) DORMANT

   prefixTARGET NODE(MIAMI1) SYSNAME(SYSTEM1) MAIN OPERATIVE

   prefixTARGET NODE(MIAMI1) SYSNAME(SYSTEM2) OPERATIVE
          PREFIX(...) PROTOCOL(...) WORKSPACE(...)
   ```

   Add these commands to the RACF parameter library for ORLANDO.

   Remember to rerun remaining commands as noted in step 3.

On MIAMI2:

1. Issue a TARGET command from the operator's console to define the connection with ORLANDO.

   ```
   prefixTARGET NODE(ORLANDO) OPERATIVE
   PREFIX(...) PROTOCOL(...) WORKSPACE(...)
   ```

   Add this command to the RACF parameter library for SYSTEM2.

   Note: The TARGET commands for SYSTEM1 and SYSTEM2 are now identical. If you want, you can now use a single RACF parameter library member for the TARGET commands for the multisystem node MIAMI1.

Glossary

A

access. The ability to obtain the use of a protected resource.

access authority. An authority related to a request for a type of access to protected resources. In RACF, the access authorities are NONE, EXECUTE, READ, UPDATE, CONTROL, and ALTER.

accessor environment element (ACEE). A description of the current user, including user ID, current connect group, user attributes, and group authorities. An ACEE is constructed during user identification and verification.

ACEE. See *accessor environment element*.

appropriate privileges. In the OpenEdition MVS implementation, superuser authority. A trusted or privileged attribute is an attribute associated with a started procedure address space and with any process associated with the address space.

AUDIT request. The issuing of the RACROUTE macro with REQUEST=AUDIT specified. An AUDIT request is a general-purpose security-audit request that can be used to audit a specified resource name and action.

AUTH request. The issuing of the RACROUTE macro with REQUEST=AUTH specified. The primary function of an AUTH request is to check a user's authorization to a RACF-protected resource or function. The AUTH request replaces the RACHECK function. See also *authorization checking*.

authority. The right to access objects, resources, or functions. See *access authority, class authority,* and *group authority*.

authorization checking. The action of determining whether a user is permitted access to a protected resource. RACF performs authorization checking as a result of a RACROUTE REQUEST=AUTH or RACROUTE REQUEST=FASTAUTH.

automatic command direction. An extension of command direction that causes RACF to automatically direct certain commands to one or more remote nodes after running the commands on the issuing node. Commands can be automatically directed based on who issued the command, the command name, or the profile class related to the command. Profiles in the RRSFDATA class control to which commands are automatically directed when automatic direction is active. See also *automatic password direction* and *command direction*.

automatic direction. An RRSF function that automatically directs commands and password-related updates to one or more remote systems. See also *automatic command direction* and *automatic password direction*.

automatic password direction. An extension of password synchronization and automatic command direction that causes RACF to automatically change the password for a user ID on one or more remote nodes after the password for that user ID is changed on the local node. Profiles in the RRSFDATA class control for direction are active. See also *password synchronization, automatic command direction*, and *automatic direction*.

C

cache structure. A coupling facility structure that contains data accessed by systems in a sysplex. MVS provides a way for multiple systems to determine the validity of copies of the cache structure data in their local storage.

callable service. In OpenEdition MVS, a request by an active process for a service. Synonymous with *syscall*, *system call*.

CDT. See *class descriptor table*.

class. A collection of RACF-defined entities (users, groups, and resources) with similar characteristics. The class names are USER, GROUP, DATASET, and the classes that are defined in the class descriptor table.

class authority (CLAUTH). An authority enabling a user to define RACF profiles in a class defined in the class descriptor table. A user can have class authorities to one or more classes.

class descriptor table (CDT). A table consisting of an entry for each class except the USER, GROUP, and DATASET classes. The table is generated by executing the ICHERCDE macro once for each class. The class descriptor table contains both the IBM provided classes and also the installation defined classes.

CLAUTH. See *class authority*.

command direction. A RRSF function that allows a user to issue a command from one user ID and direct that command to run under the authority of a different

user ID on the same or a different RRSF node. Before a command can be directed from one user ID to another, a user ID association must be defined between them via the RACLINK command.

command interpreter. A program that reads the commands that you type in and then executes them. When you are typing commands into the computer, you are actually typing input to the command interpreter. The interpreter then decides how to perform the commands that you have typed. The shell is an example of a command interpreter. Synonymous with *command language interpreter*. See also *shell*.

command language interpreter. Synonym for *command interpreter*.

coupling facility. The hardware element that provides high-speed caching, list processing, and locking functions in a sysplex.

D

Data Facility Product (DFP). A program that isolates applications from storage devices, storage management, and storage device hierarchy management.

data security. The protection of data from unauthorized disclosure, modification, or destruction, whether accidental or intentional.

data security monitor (DSMON). A RACF auditing tool that produces reports enabling an installation to verify its basic system integrity and data-security controls.

data set profile. A profile that provides RACF protection for one or more data sets. The information in the profile can include the data-set profile name, profile owner, universal access authority, access list, and other data. See *discrete profile* and *generic profile*.

data sharing mode. An operational RACF mode that is available when RACF is enabled for sysplex communication. Data sharing mode uses global resource serialization protocol that allows concurrent RACF instances to directly access and change the same database while maintaining data integrity as always. Data sharing mode requires installation of coupling facility hardware.

default group. In RACF, the group specified in a user profile that is the default current connect group.

DEFINE request. The issuing of the RACROUTE macro with REQUEST=DEFINE specified. Also, using a RACF command to add or delete a resource profile causes a DEFINE request. The DEFINE request replaces the RACDEF function.

DFP. See Data Facility Product.

DFP segment. The portion of a RACF profile containing information relating to the users and resources that are managed by the data facility product (DFP).

DIRAUTH request. The issuing of the RACROUTE macro with REQUEST=DIRAUTH specified. A DIRAUTH request works on behalf of the message-transmission managers to ensure that the receiver of a message meets security-label authorization requirements.

directed command. A RACF command that is issued from a user ID on an RRSF node. It runs in the RACF subsystem address space on the same or a different RRSF node under the authority of the same or a different user ID. A directed command is one that specifies AT or ONLYAT. See also *command direction* and *automatic command direction*.

directory. (1) A type of file containing the names and controlling information for other files or other directories. (2) A construct for organizing computer files. As files are analogous to folders that hold information, a directory is analogous to a drawer that can hold a number of folders. Directories can also contain subdirectories, which can contain subdirectories of their own. (3) A file that contains directory entries. No two directory entries in the same directory can have the same name. (4) A file that points to files and to other directories. (5) An index used by a control program to locate blocks of data that are stored in separate areas of a data set in direct access storage.

discrete profile. A resource profile that can provide RACF protection for only a single resource. For example, a discrete profile can protect only a single data set or minidisk.

DSMON. See *data security monitor*.

E

entity. A user, group, or resource (for example, a DASD data set) that is defined to RACF.

EXTRACT request. The issuing of the RACROUTE macro with REQUEST=EXTRACT specified. An EXTRACT request retrieves or replaces certain specified fields from a RACF profile or encodes certain clear-text (readable) data. The EXTRACT request replaces the RACXTRT function.

F

FASTAUTH request. The issuing of the RACROUTE macro with REQUEST=FASTAUTH specified. The primary function of a FASTAUTH request is to check a user's authorization to a RACF-protected resource or function. A FASTAUTH request uses only in-storage profiles for faster performance. The FASTAUTH request replaces the FRACHECK function. See also *authorization checking*.

G

general resource. Any system resource, other than an MVS data set, that is defined in the class descriptor table (CDT). General resources are DASD volumes, tape volumes, load modules, terminals, IMS and CICS transactions, and installation-defined resource classes.

general resource profile. A profile that provides RACF protection for one or more general resources. The information in the profile can include the general resource profile name, profile owner, universal access authority, access list, and other data.

general-use programming interface (GUPI). An interface that IBM makes available for use in customer-written programs with few restrictions and that does not require knowledge of the detailed design or implementation of the IBM software product. See also *product-sensitive programming interface (PSPI)*.

generic profile. A resource profile that can provide RACF protection for one or more resources. The resources protected by a generic profile have similar names and identical security requirements. For example, a generic data-set profile can protect one or more data sets.

GID. See *group identifier*.

group. A collection of RACF-defined users who can share access authorities for protected resources.

group authority. An authority specifying which functions a user can perform in a group. The group authorities are USE, CREATE, CONNECT, and JOIN.

group identifier (GID). (1) In OpenEdition MVS, a unique number assigned to a group of related users. The GID can often be substituted in commands that take a group name as an argument. (2) A non-negative integer, which can be contained in an object of type *gid_t,* that is used to identify a group of system users. Each system user is a member of at least one group. When the identity of a group is associated with a process, a group ID value is referred to as a real group ID, an effective group ID, one of the (optional) supplementary group IDs, or an (optional) saved set-group-ID.

group profile. A profile that defines a group. The information in the profile includes the group name, profile owner, and users in the group.

GUPI. See *general-use programming interface*.

H

HFS. See *hierarchical file system*.

hierarchical file system (HFS). Information is organized in a tree-like structure of directories. Each directory can contain files or other directories.

I

ICB. See *inventory control block*.

inventory control block (ICB). The first block in a RACF database. The ICB contains a general description of the database.

K

kernel. (1) In OpenEdition MVS, the part of an operating system that contains programs for such tasks as I/O, management, and control of hardware and the scheduling of user tasks. (2) The part of the system that is an interface with the hardware and provides services for other system layers such as system calls, file system support, and device drivers. (3) The part of an operating system that performs basic functions such as allocating hardware resources. (4) A program that can run under different operating system environments. See also *shell*. (5) A part of a program that must be in central storage in order to load other parts of the program.

L

LIST request. The issuing of the RACROUTE macro with REQUEST=LIST specified. A LIST request builds in-storage profiles for RACF-defined resources. The LIST request replaces the RACLIST function.

local logical unit (LU). Local LUs are LUs defined to the MVS system; partner LUs are defined to remote systems. It is a matter of point of view. From the point of view of a remote system, LUs defined to that system are local LUs, and those on MVS are the partner LUs.

A partner LU might or might not be on the same system as the local LU. When both LUs are on the same system, the LU through which communication is initiated

is the local LU, and the LU through which communication is received is the partner LU.

local node. The RRSF node from whose point of view you are talking. For example, if MVSA and MVSB are two RRSF nodes that are logically connected, from MVSA's point of view MVSA is the local node, and from MVSB's point of view MVSB is the local node. See also *remote node*.

logical unit. A port providing formatting, state synchronization, and other high-level services through which an end user communicates with another end user over an SNA network.

LU. See *logical unit*.

M

main system. The system on a multisystem RRSF node that is designated to receive most of the RRSF communications sent to the node.

member system. Any one of the MVS system images in a multisystem RRSF node.

multisystem node. See *multisystem RRSF node*

multisystem RRSF node. An RRSF node consisting of multiple MVS system images that share the same RACF database. One of the systems is designated to be the main system, and it receives most of the RRSF communications sent to the node.

MVS. Multiple virtual storage. Implies MVS/370, MVS/XA, and MVS/ESA.

N

NetView segment. The portion of a RACF profile containing NetView logon information.

node. See RRSF node.

O

OVM segment. The portion of a RACF profile containing OVM logon information.

owner. The user or group who creates a profile, or is named the owner of a profile. The owner can modify, list, or delete the profile.

P

partner logical unit (partner LU). Partner LUs are LUs defined to remote systems; LUs defined to the MVS system are local LUs. It is a matter of a point of view. From the point of view of the remote system, LUs defined to that system are local LUs, and the ones on MVS are the partner LUs.

A partner LU might or might not be on the same system as the local LU. When both LUs are on the same system, the LU through which communication is initiated is the local LU, and the LU through which communication is received is the partner LU.

PassTicket. An alternative to the RACF password that permits workstations and client machines to communicate with the host. It allows a user to gain access to the host system without sending the RACF password across the network.

password. In computer security, a string of characters known to the computer system and a user, who must specify it to gain full or limited access to a system and to the data stored within it. In RACF, the password is used to verify the identity of the user.

password synchronization. An option which can be specified when a peer user ID association is defined between two user IDs. If password synchronization is specified for a user ID association, then whenever the password for one of the associated user IDs is changed, the password for the other user ID is automatically changed to the newly defined password. See also *automatic password direction*.

permission bits. In OpenEdition MVS, part of security controls for directories and files stored in the hierarchical file system (HFS). Used to grant read, write, search (just directory), or execute (just file) access to owner, owner's group, or all others.

posit. A number specified for each class in the class descriptor table that identifies a set of flags that control RACF processing options. See the keyword description for posit in *OS/390 Security Server (RACF) Macros and Interfaces*.

process. (1) A function being performed or waiting to be performed. (2) An executing function, or one waiting to execute. (3) A function, created by a **fork()** request, with three logical sections:

- Text, which is the function's instructions.
- Data, which the instructions use but do not change.
- Stack, which is a push-down, pop-up save area of the dynamic data that the function operates upon.

The three types of processes are:

- User processes, which are associated with a user at a workstation

- Daemon processes, which do systemwide functions in user mode, such as printer spooling
- Kernel processes, which do systemwide functions in kernel mode, such as paging

A process can run in an OpenEdition user address space, an OpenEdition forked address space, or an OpenEdition kernel address space. In an MVS system, a process is handled like a task. See also *task*. (4) An address space and one or more threads of control that execute within that address space, and their required system resources. (5) An address space and single thread of control that executes within that address space, and its required system resources. A process is created by another process issuing the **fork()** function. The process that issues **fork()** is known as the parent process, and the new process created by the **fork()** is known as the child process. (6) A sequence of actions required to produce a desired result. (7) An entity receiving a portion of the processor's time for executing a program. (8) An activity within the system that is started by a command, a shell program, or another process. Any running program is a process. (9) A unique, finite course of events defined by its purpose or by its effect, achieved under given conditions. (10) Any operation or combination of operations on data. (11) The current state of a program that is running—including a memory image, the program data, the variables used, the general register values, the status of opened files used, and the current directory. Programs running in a process must be either operating system programs or user programs. (12) A running program, including the memory occupied, the open files, the environment, and other attributes specific to a running program.

product-sensitive programming interface (PSPI). A programming interface intended to be used only for specialized tasks such as: diagnosis, modification, monitoring, repairing, tailoring, and tuning of the IBM software product and that depends on or requires the customer to understand significant aspects of the design and implementation of the IBM software product. See also *general-use programming interface (GUPI)*.

profile. Data that describes the significant characteristics of a user, a group of users, or one or more computer resources. See also *data set profile, discrete profile, general resource profile, generic profile, group profile,* and *user profile*.

program access to data sets (PADS). A RACF function that enables an authorized user or group of users to access one or more data sets at a specified access authority only while running a specified RACF-controlled program. See also *program control*.

program control. A RACF function that enables an installation to control who can run RACF-controlled programs. See also *program access to data sets*.

PSPI. See *product-sensitive programming interface*.

R

RACF. See Resource Access Control Facility.

RACF database. A collection of interrelated or independent data items stored together without unnecessary redundancy, to serve Resource Access Control Facility (RACF).

RACF remote sharing facility (RRSF). RACF services that function within the RACF subsystem address space to provide network capabilities to RACF.

RACF remove ID utility. A RACF utility which identifies references to user IDs and group IDs in the RACF database. The utility can be used to find references to residual user IDs and group IDs or specified user IDs and group IDs. The output from this utility is a set of RACF commands that can be used to remove the references from the RACF database after review and possible modification by the customer.

RACF report writer. A RACF function that produces reports on system use and resource use from information found in the RACF SMF records.

RACF SMF data unload utility. A RACF utility that enables installations to create a sequential file from the security relevant audit data. The sequential file can be used in several ways: viewed directly, used as input for installation-written programs, and manipulated with sort/merge utilities. It can also be uploaded to a database manager (for example, DB2) to process complex inquiries and create installation-tailored reports.

RACF-protected. Pertaining to a resource that has either a discrete profile, an applicable generic profile, or a file or directory that doesn't have a profile, but is protected with the File Security Packet (FSP). A data set that is RACF-protected by a discrete profile must also be RACF-indicated.

RACROUTE macro. An assembler macro that provides a means of calling RACF to provide security functions. See also *AUDIT request, AUTH request, DEFINE request, DIRAUTH request, EXTRACT request, FASTAUTH request, LIST request, SIGNON request, STAT request, TOKENBLD request, TOKENMAP request, TOKENXTR request, VERIFY request,* and *VERIFYX request*.

remote logical unit (remote LU). See *partner logical unit (partner LU)*. These two terms are interchangeable.

remote node. An RRSF node that is logically connected to a node from whose point of view you are talking. For example, if MVSX and MVSY are two

RRSF nodes that are logically connected, from MVSX's point of view MVSY is a remote node, and from MVSY's point of view MVSX is a remote node. See also *local node*, *target node*.

Resource Access Control Facility (RACF). An IBM-licensed product that provides for access control by identifying and verifying users to the system, authorizing access to protected resources, logging detected unauthorized attempts to enter the system, and logging detected accesses to protected resources.

resource profile. A profile that provides RACF protection for one or more resources. User, group, and connect profiles are not resource profiles. The information in a resource profile can include the data set profile name, profile owner, universal access authority, access list, and other data. Resource profiles can be discrete profiles or generic profiles. See *discrete profile* and *generic profile*.

root. (1) The starting point of the file system. (2) The first directory in the system. (3) See *appropriate privileges*.

RRSF. See *RACF remote sharing facility*.

RRSF logical node connection. Two RRSF nodes are logically connected when they are properly configured to communicate via APPC/MVS, and they have each been configured via the TARGET command to have an OPERATIVE connection to the other.

RRSF network. Two or more RRSF nodes that have established RRSF logical node connections to each other.

RRSF node. One or more MVS system images with MVS/ESA 4.3 or later installed, RACF 2.2 installed, and the RACF subsystem address space active. See also *RRSF logical node connection*.

S

SAF. System authorization facility.

security. See *data security*.

security classification. The use of security categories, a security level, or both, to impose additional access controls on sensitive resources. An alternative way to provide security classifications is to use security labels.

SFS. Shared file system

shared file system (SFS). A part of CMS that lets users organize their files into groups known as directories and selectively share those files and directories with other users.

shell. (1) In OpenEdition MVS, a program that interprets and processes interactive commands from a pseudoterminal or from lines in a shell script. (2) A program that interprets sequences of text input as commands. It may operate on an input stream, or it may interactively prompt and read commands from a terminal. Synonymous with *command language interpreter*. (3) A software interface between a user and the operating system of a computer. Shell programs interpret commands and user interactions on devices such as keyboards, pointing devices and touch-sensitive screens and communicate them to the operating system. (4) The command interpreter that provides a user interface to the operating system and its commands. (5) The program that reads a user's commands and executes them. (6) The shell command language interpreter, a specific instance of a shell. (7) A layer, above the kernel, that provides a flexible interface between users and the rest of the system. (8) Software that allows a kernel program to run under different operating system environments.

SIGNON request. The issuing of the RACROUTE macro with REQUEST=SIGNON specified. A SIGNON request is used to provide management of the signed-on lists associated with persistent verification (PV), a feature of the APPC architecture of LU 6.2.

single-system RRSF node. An RRSF node consisting of one MVS system image.

SMF records. See *RACF SMF data unload utility*.

STAT request. The issuing of the RACROUTE macro with REQUEST=STAT specified. A STAT request determines if RACF is active and optionally, whether a given resource class is defined to RACF and active. The STAT request replaces the RACSTAT function.

structure. See *cache structure*.

supervisor. The part of a control program that coordinates the use of resources and maintains the flow of processing unit operations. Synonym for *supervisory routine*.

supervisory routine. A routine, usually part of an operating system, that controls the execution of other routines and regulates the flow of work in a data processing system. Synonymous with *supervisor*.

syscall. In OpenEdition MVS, deprecated term for *callable service*.

sysplex. A set of MVS systems communicating and cooperating with each other through multisystem hardware elements and software services to process customer workloads.

sysplex communication. An optional RACF function that allows the system to use XCF services and communicate with other systems that are also enabled for sysplex communication.

system authorization facility (SAF). An MVS component that provides a central point of control for security decisions. It either processes requests directly or works with RACF or another security product to process them.

system call. In OpenEdition MVS, synonym for *callable service*.

T

target node. An RRSF node that a given RRSF node is logically connected to, as a result of a TARGET command. The local node is a target node of itself, and all of its remote nodes are target nodes. See also *local node*, *remote node*.

task. (1) A basic unit of work to be accomplished by a computer. The task is usually specified to a control program in a multiprogramming or multiprocessing environment. (2) A basic unit of work to be performed. Some examples include a user task, a server task, and a processor task. (3) A process and the procedures that run the process. (4) In a multiprogramming or multiprocessing environment, one or more sequences of instructions treated by a control program as an element of work to be accomplished by a computer. (5) The basic unit of work for the MVS system.

TOKENBLD request. The issuing of the RACROUTE macro with REQUEST=TOKENBLD specified. A TOKENBLD request builds a UTOKEN.

TOKENMAP request. The issuing of the RACROUTE macro with REQUEST=TOKENMAP specified. A TOKENMAP request maps a token in either internal or external format, allowing a caller to access individual fields within the UTOKEN.

TOKENXTR request. The issuing of the RACROUTE macro with REQUEST=TOKENXTR specified. A TOKENXTR request extracts a UTOKEN from the current address space, task or a caller-specified ACEE.

transaction program (TP). A program used for cooperative transaction processing within an SNA network. For APPC/MVS, any program on MVS that issues APPC/MVS or CPI Communication calls, or is scheduled by the APPC/MVS transaction scheduler.

TSO segment. The portion of a RACF profile containing TSO logon information.

U

UACC. See *universal access authority*.

UID. See *user identifier*.

universal access authority (UACC). The default access authority that applies to a resource if the user or group is not specifically permitted access to the resource. The universal access authority can be any of the access authorities.

user. A person who requires the services of a computing system.

user ID. A string of characters that uniquely identifies a user to a system. A user ID is 1 to 8 alphanumeric characters. On TSO, user IDs cannot exceed 7 characters and must begin with an alphabetic, #, $, or @ character.

user identification and verification. The acts of identifying and verifying a RACF-defined user to the system during logon or batch job processing. RACF identifies the user by the user ID and verifies the user by the password or operator identification card supplied during logon processing or the password supplied on a batch JOB statement.

user identifier (UID). (1) A unique string of characters that identifies an operator to the system. This string of characters limits the functions and information the operator can use. (2) A non-negative integer, which can be contained in an object of type *uid_t,* that is used to identify a system user. When the identity of the user is associated with a process, a user ID value is referred to as a real user ID, an effective user ID, or an (optional) saved set-user-ID. (3) The identification associated with a user or job. The two types of user IDs are:

- **RACF user ID:** A string of characters that uniquely identifies a RACF user or a batch job owner to the security program for the system. The batch job owner is specified on the USER parameter on the JOB statement or inherited from the submitter of the job. This user ID identifies a RACF user profile.
- **OMVS user ID:** A numeric value between 0 and 2147483647, called a UID (or sometimes a user number), that identifies a user to OpenEdition services. These numbers appear in the RACF user profile for the user.

A user ID is equivalent to an account on a UNIX-type system. (4) A symbol identifying a system user. (5) Synonymous with user identification.

user name. (1) In RACF, one to 20 alphanumeric characters that represent a RACF-defined user. (2) In

OpenEdition MVS, a string that is used to identify a user.

user profile. A description of a RACF-defined user that includes the user ID, user name, default group name, password, profile owner, user attributes, and other information. A user profile can include information for subsystems such as TSO and DFP. See *TSO segment* and *DFP segment*.

V

verification. See *user identification and verification*.

VERIFY request. The issuing of the RACROUTE macro with REQUEST=VERIFY specified. A VERIFY request is used to verify the authority of a user to enter work into the system. The VERIFY request replaces the RACINIT function.

VERIFYX request. The issuing of the RACROUTE macro with REQUEST=VERIFYX specified. A VERIFYX request verifies a user and builds a UTOKEN, and handles the propagation of submitter ID.

VM. A licensed program that controls “virtual machines” and runs on two main command languages, CP and CMS. Can be VM/SP, VM/HPO, VM/XA, or VM/ESA.

W

workspace data sets. VSAM data sets used by RACF for queuing requests sent to and received from target nodes in an RRSF environment.

Index

E

F

G

H

I

R

S

T

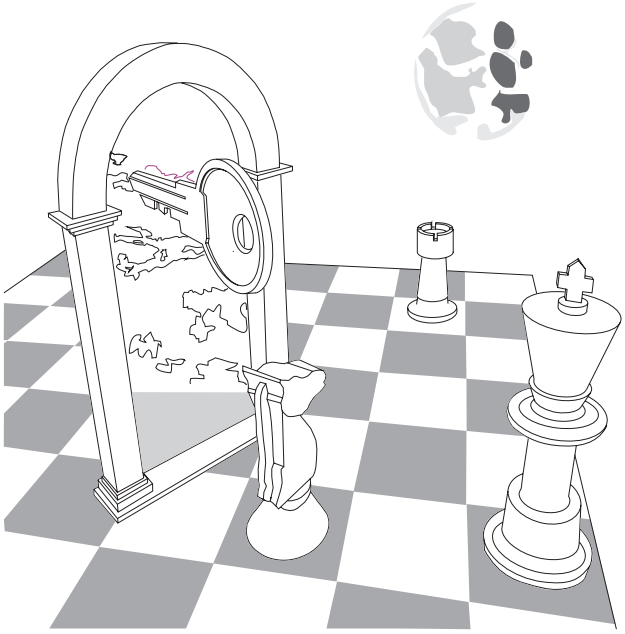
U

V

W

Y

RACF's Greatest Hits: Now on CD



Let's face it, you have to search through a ton of hardcopy manuals to locate all of the information you need to secure your entire system. There are manuals for OS/390, VM, CICS, TSO/E; technical bulletins from the International Technical Support Organization ("red books"), Washington Systems Center ("orange books"); multiple levels of OS/390 Security Server (RACF) manuals; and much more. Wouldn't it be great if you could have all of this information in one convenient package?

Now you can! The *IBM Online Library Productivity Edition OS/390 Security Server (RACF) Information Package* includes key books from a wide variety of System/390 operating system and application product libraries that refer to RACF and OS/390 Security Server (including OpenEdition DCE Security Server and RACF). You can search the information package to find all the RACF hits and hints you need.

You can view and search the books on CD-ROM at your workstation or terminal using:

- The IBM BookManager Library Reader for OS/2, DOS, or Windows**, all of which are provided at no charge with each CD-ROM
- Any of the IBM BookManager READ licensed programs for MVS[3], VM, OS/2, DOS, AIX/6000, or Windows.

The OS/390 Security Server (RACF) Information Package is available as product feature code 8004 with OS/390 or as product feature code 9006 with RACF Version 2. You can also order it through normal publication ordering channels as SK2T-2180. If you have any specific questions or if you'd like more information about this online collection, write to us at one of the following:

- ► By mail, use this form. If you are mailing this form from a country other than the United States, you can give it to the local IBM branch office or IBM representative for postage-paid mailing.
- ► By FAX, use this number: (International Access Code)+1+914+432-9405
- ► IBMLink (United States customers only): KGNVMC(MHVRCFS)
- ► IBM Mail Exchange: USIB6TC9 at IBMMAIL
- ► Internet: mhvrcfs@vnet.ibm.com

Name

Address

Company or Organization

City State Zip Code

Phone or FAX Number

E-Mail Address

3 IBM BookManager READ/MVS is part of the OS/390 product.

Communicating Your Comments to IBM

OS/390
Security Server (RACF)
Planning: Installation and Migration

Publication No. GC28-1920-01

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

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

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

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

- If you prefer to send comments by mail, use the RCF at the back of this book.
- If you prefer to send comments by FAX, use this number:
  - FAX: (International Access Code)+1+914+432-9405
- If you prefer to send comments electronically, use this network ID:
  - IBMLink: (United States customers only): KGNVMC(MHVRCFS)
  - IBM Mail Exchange: USIB6TC9 at IBMMAIL
  - Internet e-mail: mhvrcfs@vnet.ibm.com
  - World Wide Web: http://www.s390.ibm.com/os390

Make sure to include the following in your note:

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

Optionally, if you include your telephone number, we will be able to respond to your comments by phone.

Reader's Comments — We'd Like to Hear from You

OS/390
Security Server (RACF)
Planning: Installation and Migration

Publication No. GC28-1920-01

You may use this form to communicate your comments about this publication, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you. Your comments will be sent to the author's department for whatever review and action, if any, are deemed appropriate.

Note: Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.

Today's date: _____

What is your occupation?

Newsletter number of latest Technical Newsletter (if any) concerning this publication:

How did you use this publication?

[ ]	As an introduction	[ ]	As a text (student)
[ ]	As a reference manual	[ ]	As a text (instructor)
[ ]	For another purpose (explain)		

Is there anything you especially like or dislike about the organization, presentation, or writing in this manual? Helpful comments include general usefulness of the book; possible additions, deletions, and clarifications; specific errors and omissions.

Page Number: Comment:

Name	Address
Company or Organization	
Phone No.	

Reader's Comments — We'd Like to Hear from You
GC28-1920-01

Cut or Fold
Along Line

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

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

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

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Department 55JA, Mail Station P384
522 South Road
Poughkeepsie NY 12601-5400

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

GC28-1920-01

Cut or Fold
Along Line

IBM®

Program Number: 5645-001

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

Drop in
Back Cover
Image Here.

GC28-1920-01