OS/390

SecureWay Security Server RACF Introduction

GC28-1912-07

OS/390

SecureWay Security Server RACF Introduction

GC28-1912-07

Note

Before using this information and the product it supports, be sure to read the general information under “Appendix. Notices” on page 37.

Eighth Edition, September 2000

This is a major revision of GC28-1912-06.

This edition applies to Version 2 Release 10 of OS/390 (5647-A01) 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
2455 South Road
Poughkeepsie, NY 12601-5400
United States of America

FAX (United States & Canada): 1+845+432-9405
FAX (Other Countries):
Your International Access Code +1+845+432-9405

IBMLink (United States customers only): IBMUSM10(MHVRCFS)
IBM Mail Exchange: USIB6TC9 at IBMMAIL
Internet e-mail: mhvrcfs@us.ibm.com
World Wide Web: http://www.ibm.com/s390/os390/webqs.html

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.

Contents

Figures

About This Book

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

- Resource Access Control Facility (RACF)
- DCE Security Server
- OS/390 Firewall Technologies
- Lightweight Directory Access Protocol (LDAP) Server
- Open Cryptographic Enhanced Plug-ins
- SecureWay Security Server Network Authentication and Privacy Service

For information about the other components of OS/390 Security Server, see the publications related to those components.

This book gives an overview of RACF. It provides general introductory information about RACF and how you can use it. This book applies to OS/390 installations.

Who Should Use This Book

Installation managers and personnel who are responsible for system-data security and integrity will find this book particularly useful. The book assumes that you are familiar with OS/390.

How to Use This Book

RACF provides:

- System security
- Resource access control
- Auditability and accountability
- Administrative control

"Chapter 1. Achieving a Secure System Environment" on page 1 discusses present-day needs for data security and provides a basic description of RACF.

"Chapter 2. What Does RACF Do?" on page 9 describes the major RACF functions, including RACF generalization and its relationship to other products.

"Chapter 3. How You Can Use RACF" on page 25 provides a high-level discussion of how you can use the RACF functions.

Where to Find More Information

Where necessary, this book references information in other books. For complete titles and order numbers for all elements of OS/390, see *OS/390 Information Roadmap*.

Softcopy Publications

The Security Server library is available on the following CD-ROMs. The CD-ROM online library collections include the IBM Library Reader, which is a program that enables you to view the softcopy books.

SK2T-6718 *OS/390 PDF Library Collection*

This collection contains the set of unlicensed books for the current release of OS/390 in Portable Document Format (PDF) files. You can view or print these files with the Adobe Acrobat reader.

SK2T-6700 *Online Library Omnibus Edition OS/390 Collection*

This softcopy collection contains a set of unlicensed books for OS/390 and related products. The collection contains the publications for multiple releases of these products.

SK2T-2180 *Online Library OS/390 SecureWay Security Server RACF Information Package*

This softcopy collection kit contains the Security Server 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 (redbooks), and Washington System Center (WSC) books (orange books) that contain 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/ESA, CICS, and NetView. For more information, see the advertisement at the back of the book.

SK2T-2177 *IBM System/390 Redbooks Collection*

This softcopy collection contains a set of S/390 redbooks.

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

This softcopy collection contains a set of key MVS and MVS-related product books. It also includes the RACF Version 2 product libraries.

RACF Courses

The following RACF classroom courses are available:

ES840 *Implementing RACF Security for CICS/ESA and CICS/TS*

H3917 *Basics of OS/390 SecureWay Security Server RACF Administration*

H3927 *Effective RACF Administration*

H4020 *Exploiting the Features of OS/390 SecureWay Security Server RACF*

IBM provides a variety of educational offerings for RACF. For more information about classroom courses and other offerings, do any of the following:

- See your IBM representative
- 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. 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.

G320-9279	*Systems Security Publications Bibliography*
GG22-9396	*Tutorial: Options for Tuning RACF*
GG24-2539	*RACF Version 2 Release 2 Technical Presentation Guide*
GG24-3378	*DFSMS and RACF Usage Considerations*
GG24-3451	*Introduction to System and Network Security: Considerations, Options, and Techniques*
GG24-3524	*Network Security Involving the NetView Family of Products*
GG24-3585	*MVS/ESA and RACF Version 1 Release 9 Security Implementation Guide*
GG24-3970	*Elements of Security: RACF Overview - Student Notes*
GG24-3971	*Elements of Security: RACF Installation - Student Notes*
GG24-3972	*Elements of Security: RACF Advanced Topics - Student Notes*
GG24-3984	*RACF Macros and Exit Coding*
GG24-4282	*Secured Single Signon in a Client/Server Environment*
GG24-4453	*Enhanced Auditing Using the RACF SMF Data Unload Utility*
GG26-2005	*RACF Support for Open Systems Technical Presentation Guide*
GC28-1210	*System/390 MVS Sysplex Hardware and Software Migration*
SG24-4580	*RACF Version 2 Release 2 Installation and Implementation Guide*
SG24-4704	*OS/390 Security Services and RACF-DCE Interoperation*
SG24-4820	*OS/390 Security Server Audit Tool and Report Application*
SG24-5158	*Ready for e-business: OS/390 Security Server Enhancements*
SG24-5339	*The OS/390 Security Server Meets Tivoli: Managing RACF with Tivoli Security Products*

Other Sources of Information

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

IBM Discussion Areas

IBM provides the following discussion areas for RACF and security-related topics.

- **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 to provide additional information about the OS/390 library and other security-related topics:

- **OS/390 Online Library**

  To view and print online versions of the OS/390 publications, use this address:

  `http://www.ibm.com/s390/os390/bkserv/`

- **System/390 Redbooks**

The redbooks that are produced by the International Technical Support Organization (ITSO) are available at the following address:

`http://www.ibm.com/redbooks/`

- **S/390 and OS/390 Security**

  For more information about security on the S/390 platform and OS/390, including the elements that comprise the SecureWay Security Server for OS/390, use this address:

  `http://www.ibm.com/s390/security/`

- **RACF Home Page**

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

  `http://www.ibm.com/s390/racf/`

- **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 and receive postings, send a note to:

  `listserv@listserv.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, including an appropriate `Subject:` line, to:

  `racf-l@listserv.uga.edu`

- **Sample Code**

  You can get sample code, internally-developed tools, and exits to help you use RACF. This code works in our environment, at the time we make it available, 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.

  To access this code from a Web browser, go to the RACF home page and select the “Downloads” topic from the navigation bar. From the IBM RACF Downloads page, you can view and download the available samples.

  The code is also available from `ftp.s390.ibm.com` through anonymous FTP. To get access:

  1. Log in as user **anonymous**.
  2. Change the directory, as follows, to find the subdirectories that contain the sample code:

     ```
     cd os390\racf
     ```

  An announcement will be posted on RACF-L, MVSRACF, and SECURITY CFORUM whenever something is added.

  Note: Some Web browsers and some FTP clients (especially those using a graphical interface) might have problems using `ftp.s390.ibm.com` because of inconsistencies in the way they implement the FTP protocols. If you have problems, you can try the following:

  – Try to get access by using a Web browser and the links from the RACF home page.

  – Use a different FTP client. If necessary, use a client that is based on command line interfaces instead of graphical interfaces.

– If your FTP client has configuration parameters for the type of remote system, configure it as UNIX instead of MVS.

Restrictions

Because the sample code and tools are not officially supported,

– There are no guaranteed enhancements.

– No APARs can be accepted.

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 *Online Library OS/390 SecureWay Security Server RACF Information Package.*

Summary of Changes

Summary of Changes
for GC28-1912-07
OS/390 Version 2 Release 10

This book contains information previously presented in *OS/390 Security Server (RACF) Introduction*, GC28-1912-06, which supports OS/390 Version 2 Release 8 and Release 9.

New Information

- Chapter 2. What Does RACF Do? contains information that describes application identity mapping and the SecureWay Security Server Network Authentication and Privacy Service.

Changed Information

- The types of DASD data sets RACF protects has been updated.

This book includes terminology, maintenance, and editorial changes, including the following:

The OS/390 Security Server, of which RACF is a component, has joined the IBM SecureWay family of products. As such, occurrences of OS/390 Security Server have been changed to SecureWay Security Server for OS/390, or its abbreviated name, Security Server. OS/390 Security Server may continue to appear in messages, panel text, and other code with SecureWay Security Server for OS/390.

Technical changes or additions to the text are indicated by a vertical line to the left of the change.

Summary of Changes
for GC28-1912-06
OS/390 Version 2 Release 8

This book contains information previously presented in *OS/390 Security Server (RACF) Introduction*, GC28-1912-05, which supports OS/390 Version 2 Release 6 and Release 7.

New Information

- Chapter 2. What Does RACF Do? contains information that describes generic ID mapping and the DFSORT ICETOOL utility
- OS/390 UNIX System Services information includes updates for protected user ID.

Changed Information

- An illustration of RACF profile checking has been added to the system authorization facility (SAF) information.
- An illustration showing how RACF provides security has been added to Chapter 2. What Does RACF Do?.
- Information on auditing a superuser has been updated.

Summary of Changes
for GC28-1912-05
OS/390 Version 2 Release 6

This book contains information previously presented in *OS/390 Security Server (RACF) Introduction*, GC28-1912-04, which supports OS/390 Version 2 Release 5.

New Information

- Additional information about RACF support for Tivoli products has been added.
- Support for the Component Broker for OS/390 has been added.

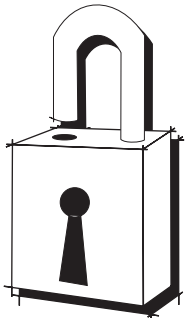
Changed Information

- As part of the name change of OpenEdition to OS/390 UNIX System Services, occurrences of OS/390 OpenEdition have been changed to OS/390 UNIX System Services or its abbreviated name, OS/390 UNIX.

Chapter 1. Achieving a Secure System Environment

The RACF component of the OS/390 Security Server works together with the existing system features of OS/390 to provide improved data security for an installation and provides Year 2000 support.

Why Security?



Advances in easy-to-use, high-level-inquiry languages, the use of small computers, and general familiarity with data processing have created a higher level of "computer literacy." Without better awareness of good data-security practices, these advances could result in a higher likelihood of unauthorized persons accessing, modifying, or destroying data, either inadvertently or deliberately. In parallel, there are two additional trends: the continuing need for information to be on some sort of database that is easily accessible by authorized users, and the increase in critical assets stored on databases.

As these and other trends continue, the need for data security takes on a new level of importance. You need to actively pursue and demonstrate security and use a security mechanism to control any form of access to critical data.

The Benefits of Security

A security mechanism should:	***How it benefits you:***
• Identify users who wish to access the secured system.	• Lets you associate a unique identifier with each potential user of the system when the user enters the system.
• Verify that the users are who they say they are.	• Provides a further level of identification, such as a *password* or *PassTicket*, to verify that the user has the correct identifier upon accessing the system.
• Allow only authorized users to access the protected resources.	• Gives users the appropriate level of access authority for each protected resource.
• Allow a convenient way to administer security.	• Allows you to select the kind of security structure and administration to use at your installation.
• Record accesses to protected resources.	• Provides another level of accountability so you can see who is using what resources. • Allows you to define the records you require.
• Document violations immediately or as a user-requested periodic report.	• Lets you see the violations whenever you want in the format you choose.
• Be usable by anyone whose data is being protected.	• Is easy to define and easy to use. This helps to prevent circumventing the mechanism.
• List the key protected resources and the level of protection that exists for each.	• Allows you to see how each resource is protected.

How RACF Meets Your Security Needs

RACF helps meet the need for security by providing:
- Flexible control of access to protected resources
- Protection of installation-defined resources
- Ability to store information for other products

- Choice of centralized or decentralized control of profiles
- An ISPF panel interface
- Transparency to end users
- Exits for installation-written routines

Because the security requirements at every data processing installation differ, these items allow you to meet your unique security objectives.

Flexible Control

RACF allows you to set your own rules for controlling access to your installation's resources by defining what is protected at what level and determining who can access protected resources. Because of RACF's flexible design, you can tailor RACF to interact with your installation's present operating environment. Because you establish the controls—while RACF enforces them—you can also adapt RACF to your changing security needs.

The RACF remote sharing facility gives you the flexibility to move work from one system to another easily.

Protection of Installation-Defined Resources

In addition to the predefined resources, such as data sets, minidisks, terminals, and transactions defined to IMS/ESA and CICS/ESA, RACF permits you to protect your own installation-defined resources. Installation-defined resources provide a great deal of flexibility in defining what resources an installation can protect.

In a system-managed storage environment, RACF allows a storage administrator to control the use of data, management, and storage classes.

Ability to Store Information for Other Products

RACF provides a repository for information needed by other products when that information relates to users or resources those products deal with. For example, RACF can store information:

- In user profiles for use by TSO/E, OS/390 UNIX System Services (OS/390 UNIX), and NetView, to name a few.
- In data set, group, and user profiles for use by DFSMS (Data Facility Storage Management Subsystem).
- In general-resource profiles for use by Hiperbatch or VTAM.

One aspect of the flexibility of RACF is the ability of the security administrator to delegate responsibility for maintaining this information to other administrators on the system. For example, the information used by DFSMS can be placed under the control of the storage administrator.

For a list of other products RACF supports, see "How RACF Supports Other Products" on page 17.

Choice of Centralized or Decentralized Control

RACF, through its ability to delegate responsibilities, allows you to assign security responsibilities on an enterprise-wide, system-wide, or group-wide basis. The RACF remote sharing facility permits you to update the RACF databases of several systems at the same time. You can administer these systems from a central location if you wish. RACF also allows different users to perform different security tasks, such as auditing and security administration.

ISPF Panels

RACF administration functions have ISPF (Interactive System Productivity Facility) entry panels and associated help panels. These panels make it easy to enter the RACF commands and their options.

Transparency to Users

No one using a data-processing system wants someone else to read or alter their data, except when they specifically intend this to happen. Unfortunately, many people hesitate to take steps to protect their data. In many cases, it is easier to ignore security procedures than to use them.

Even conscientious users can forget to protect a critical piece of data. The solution to implementing effective security measures is to provide a security system that is transparent to the user.

With RACF, end users do not need to be aware that RACF is protecting their data. By using RACF's administrative capabilities, you can make RACF transparent to most of its end users.

Exits for Installation-Written Routines

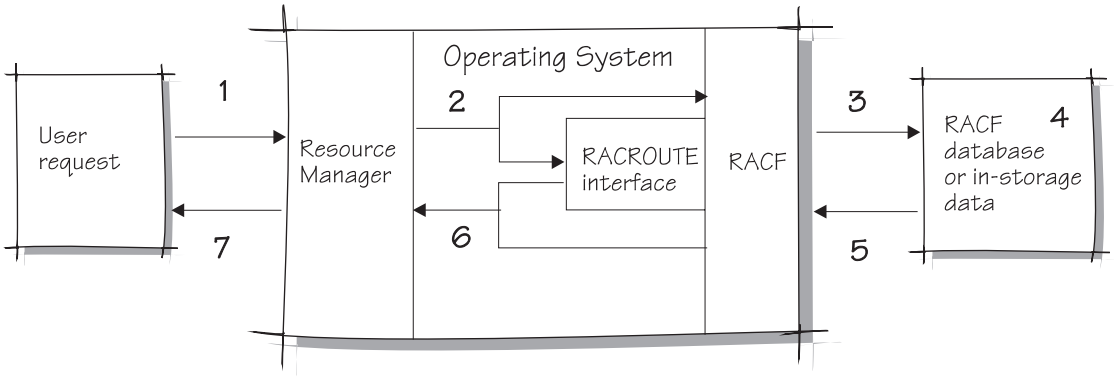
RACF allows you to write your own exit routines to deal with the unique security needs of your installation. These exit routines can be associated with the RACF commands, or they can deal with authorization checking or user passwords.

How RACF Works with the Operating System

To visualize how RACF works, picture RACF as a layer in the operating system that verifies users' identities and grants user requests to access resources.

Assume, for example, that you have been identified and verified to the RACF-protected system and now want to modify an existing RACF-protected resource. After you enter a command to the system to access the resource, a system resource manager (such as data management) processes the request. The resource manager, based on what RACF indicates, either grants or denies the request.

Figure 1 on page 4 shows how RACF interacts with the operating system to allow access to a protected resource. The operating system interacts with RACF in a similar manner to identify and verify users.



1. A user requests access to a resource using a resource manager (for example, TSO/E).
2. The resource manager issues a RACF request to see if the user can access the resource.
3. RACF refers to the RACF database or in-storage data and...
4. ...checks the appropriate resource profile.
5. Based on the information in the profile...
6. RACF passes the status of the request to the resource manager.
7. The resource manager grants (or denies) the request.

Figure 1. RACF and Its Relationship to the Operating System

During authorization checking, RACF checks the resource profile to ensure that the resource can be accessed in the way requested and that you have the proper authorization to access the resource. The necessary user-resource requirements must match before RACF grants the access request to a protected resource.

Figure 2 illustrates a conceptual model of how RACF checks profiles to ensure *who* (in a user profile) is accessing *what* and *how* (in a resource profile).

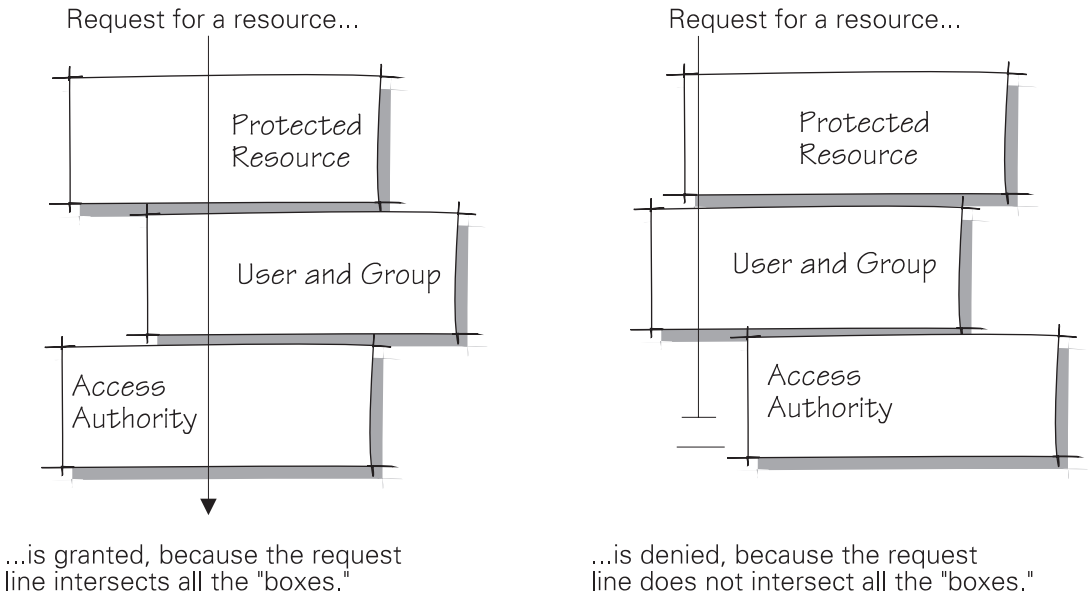


Figure 2. Conceptual Illustration of RACF Profile Checking

The “boxes” refer to the installation-assigned attributes and authorities for users and resources that determine which users can access which resources in what manner.

System Authorization Facility

The system authorization facility (SAF) is part of the operating system and conditionally directs control to RACF, if RACF is present, or to a user-supplied processing routine, or both, when receiving a request from a **resource manager**.

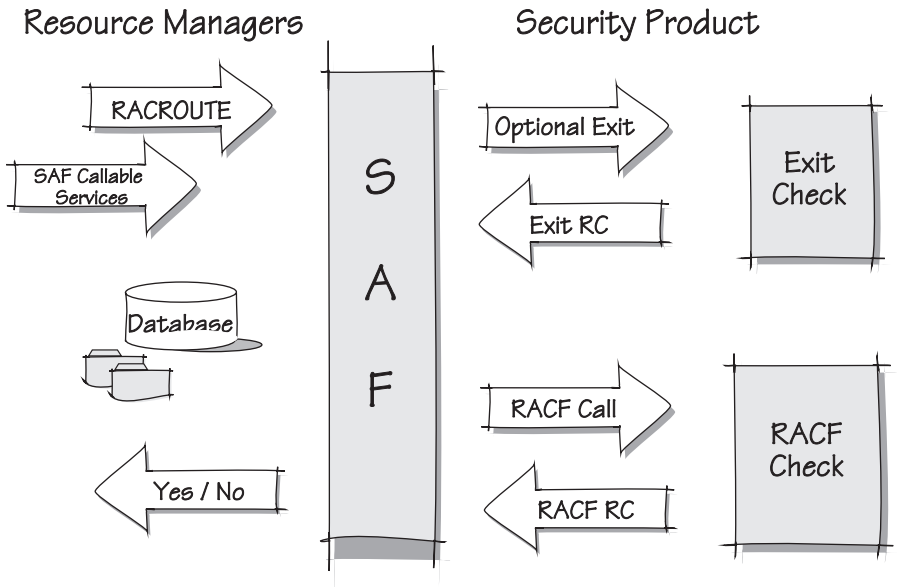


Figure 3. Conceptual Illustration of RACF Profile Checking

SAF does not require any other product as a prerequisite, but overall system security functions are greatly enhanced and complemented if it is used concurrently with RACF. The key element in SAF is the SAF router. The SAF router is always present, even when RACF is not present.

The SAF router is a system service that provides a common focal point for all products providing resource control. This focal point encourages the use of common control functions shared across products and across systems. The resource-managing components and subsystems call the MVS router as part of certain decision-making functions in their processing, such as access-control checking and authorization-related checking. These functions are called **control points**.

RACF Sysplex Data Sharing

In an MVS sysplex with many systems sharing the RACF database, problems can arise in the areas of system performance, management, and availability. RACF sysplex data sharing addresses these problems with:

- Sysplex command propagation
- The coupling facility

Sysplex Command Propagation

When you issue the RVARY command or certain SETROPTS commands on one system, RACF communicates the command throughout the sysplex. You do not need to issue the command on every system.

If hardware or software problems require you to switch to the backup database, you can do so with a single RVARY command and a single response to an operator prompt. RACF switches all the systems in the sysplex, giving them immediate access to the backup database.

Regardless of whether the coupling facility is in use, sysplex data sharing allocates local buffers to backup data sets. The use of local buffers can improve performance during I/O to the backup data sets.

Sysplex Data Sharing Restrictions:

- Although you can use sysplex data sharing on MVS/ESA 4.2 or later systems, data sharing mode requires all systems in the sysplex to be at MVS/ESA 5.1 or later.
- Sysplex data sharing does not coexist with versions of RACF earlier than version 2.1 or with RACF on VM. Systems running with sysplex communication enabled in non-data sharing mode can share a database with earlier RACF systems or with VM systems.
- Although data sets cannot be shared, you can share data outside the sysplex by using the RACF remote sharing facility.

The Coupling Facility

RACF sysplex data sharing uses the coupling facility to improve performance. When the system is in **data sharing mode**, the coupling facility provides a large central buffer for RACF database records. The large buffer can hold more of each system's database than the system's own small local buffer, and permits you to share the buffered information with other systems.

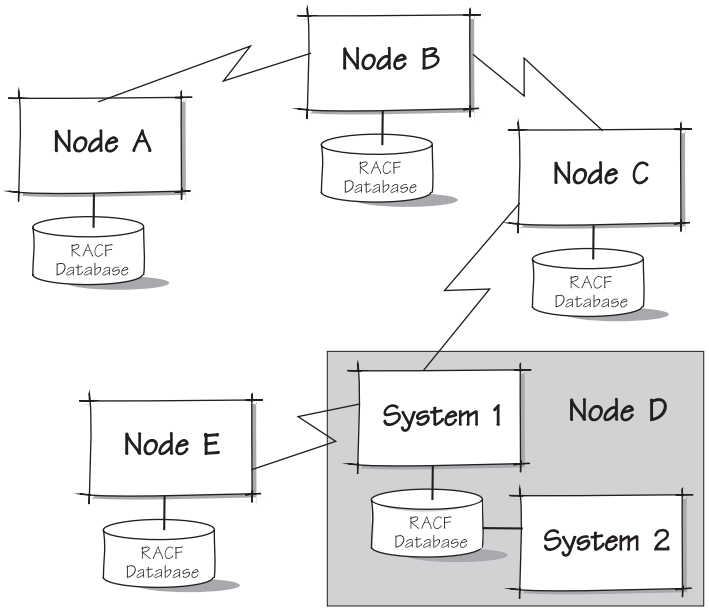
Data sharing mode is only part of sysplex data sharing. When the system is in data sharing mode, the coupling facility is installed and available. A system enabled for sysplex data sharing can perform data sharing functions that do not require the coupling facility, such as sysplex command propagation, regardless of whether the system is in data sharing mode.

RACF Remote Sharing Facility (RRSF)

The RACF remote sharing facility (RRSF) allows you to administer and maintain RACF databases that are distributed throughout the enterprise. It provides improvements in system performance, system management, system availability, and usability. RRSF helps to ensure that data integrity is kept across system or network failures and delays. It lets you know when key events have occurred and returns output to view at your convenience. A wealth of SAMPLIB materials makes it easy to setup and use common RRSF configurations and options.

RRSF Nodes

The RRSF network consists of a collection of nodes. Each node consists of one or more MVS system images and uses a specific RACF database. All RRSF nodes work in local or remote mode, depending on how they're configured.



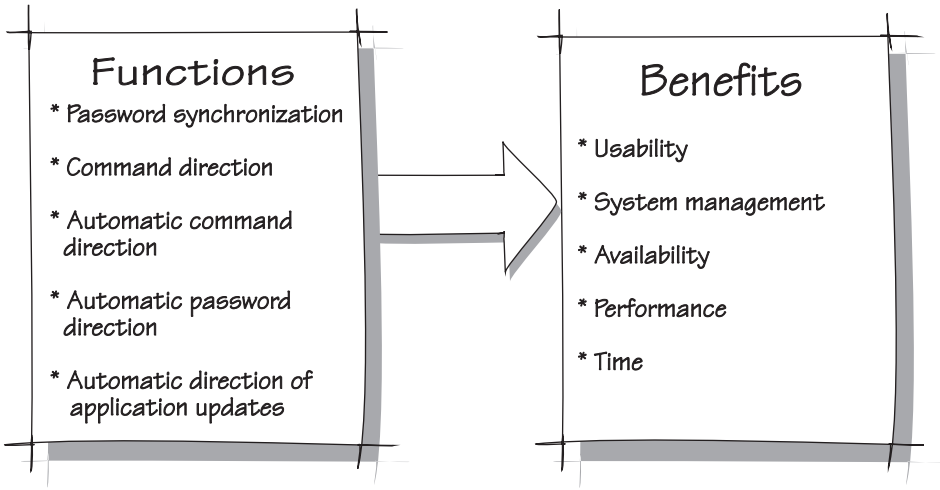
In this example of an RRSF network:

- Nodes A, B, C, and E are MVS systems with their own RACF databases. They are **single-system nodes**.
- Node D consists of two MVS systems sharing a RACF database. It is a **multisystem node**.

If you are at **Node A**, all other nodes are considered to be **remote nodes**, and Node A is known as the **local node**. RRSF allows you to administer both the local and remote nodes.

Remote Administration

The RRSF environment gives you the ability to administer remote systems. With RRSF, you can perform several functions.



- **Password synchronization**

  In a remote sharing environment, you can ask RACF to synchronize passwords for specific user IDs. When you change one password, RACF can change the passwords for your user ID on different nodes or for several user IDs on the same node. This provides improved usability.
- **Command direction**

  Command direction allows you to issue the same command on multiple databases and to send a command from one system to another. For example, if several systems need the same database information and you are not using automatic command direction, you can administer several RACF databases from a central location. This provides improved usability because administrators no longer need to logon to multiple systems.
- **Automatic command direction**

  Automatic command direction allows you to issue the same command on multiple databases automatically. It improves availability and performance by enabling you to use separate databases that are synchronized to contain the same information.

  It is especially useful in recovery or back-up situations or when you want the same database contents but cannot share physical DASD.
- **Automatic direction of application updates**

  Automatic direction of application updates allows you to automatically propagate RACF database updates made by applications. It is related to automatic command direction and improves availability and performance by enabling you to use separate databases that are synchronized to contain the same information.
- **Automatic password direction**

  Automatic password direction allows you to change passwords for the same user ID on different nodes automatically. If you used automatic password direction with automatic command direction, it improves availability and performance by keeping several databases synchronized with the same password information.

Chapter 2. What Does RACF Do?

RACF protects resources by granting access *only* to authorized users of the protected resources. RACF retains information about the users, resources, and access authorities in **profiles** on the **RACF database** and refers to the profiles when deciding which users should be permitted access to protected system resources.

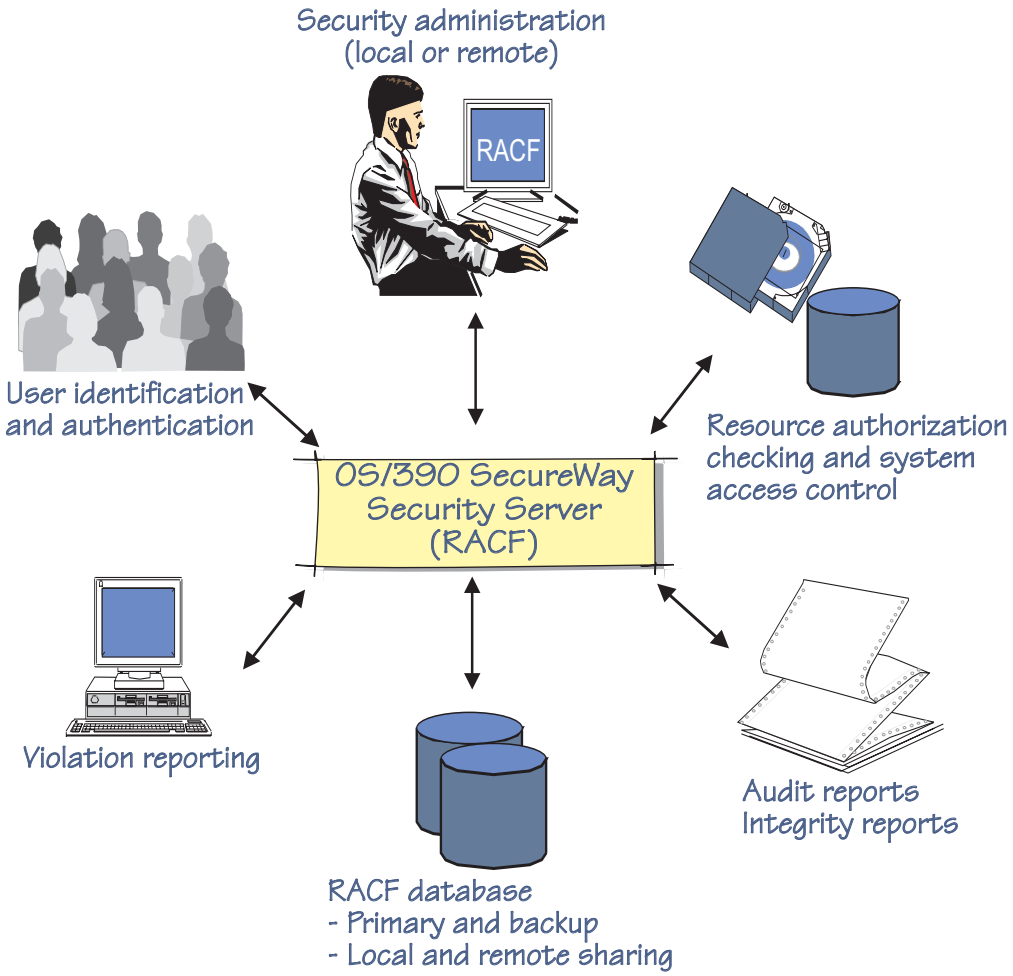


Figure 4. How RACF Provides Security

To accomplish its goals, RACF gives you the ability to:

- Identify and authenticate users
- Authorize users to access the protected resources
- Log and report various attempts of unauthorized access to protected resources
- Control the means of access to resources
- Allow applications to use the RACF macros

Identifying and Authenticating Users

For a software access control mechanism to work effectively, it must be able to:

1. **Identify** the person who is trying to gain access to the system
2. **Authenticate** the user by verifying that the user is really that person

RACF uses a **user ID** to identify the person who is trying to gain access to the system and a **password** to authenticate that identity. RACF uses the concept of only one person knowing a particular user ID and password combination to verify user identities and to ensure personal accountability.

Alternatives to Passwords:

1. RACF allows workstations and client machines in a client-server environment to use a PassTicket in place of a password. A PassTicket can be generated by RACF or by another authorized function, and can be used only once on a given computer system, within ten minutes of generation.
2. RACF allows the use of an operator identification card (OIDCARD) in place of or in addition to the password during terminal processing. By requiring that a person not only know a password but also furnish an OIDCARD, an installation has increased assurance that the user ID has been entered by the proper user.
3. OS/390 UNIX users are also identified with numeric OS/390 UNIX user identifiers (UIDs), and OS/390 UNIX groups are identified with numeric OS/390 UNIX group identifiers (GIDs). Unlike user names or group names, these numeric IDs can be shared by more than one user or group, although sharing is not recommended.
4. RACF allows you to create a protected user ID that can be used for OS/390 UNIX, UNIX daemons, and other started tasks without using a password. The protected user ID cannot be used to access a system by any means that normally requires a password, such as TSO/E logon, CICS sign on, OS/390 UNIX rlogin, or batch job submission, and cannot be used with a password. This protects the user ID from being revoked if an incorrect password is entered.
5. In a client/server environment, RACF can identify a RACF user ID by extracting information from the digital certificate. A digital certificate or digital ID, issued by a certifying authority, contains information that uniquely identifies the client.

   The WebSphere Application Server authenticates a client using the client's certificate and the Secure Sockets Layer (SSL) protocol. The server passes the client's digital certificate to OS/390 UNIX for validation. OS/390 UNIX passes the certificate to RACF. This means that the RACF user ID and password of each client do not need to be supplied when accessing secure Web pages.

RACF identifies and authenticates users accessing the system when the various system resource managers (such as job initiation) request it. RACF determines:

- If the user is defined to RACF
- If the user has supplied a valid password, PassTicket, or operator identification card (OIDCARD), and a valid group name
- If the user's UID and GID are valid on OS/390 UNIX.

- If the user ID is in REVOKE status, which prevents a RACF-defined user from entering the system at all or entering the system with certain groups
- If the user can use the system on this day and at this time of the day (an installation can impose restrictions)
- If the user is authorized to access the terminal (which can also include day and time restrictions for accessing that terminal)
- If the user is authorized to access the application

After it has authenticated the user's identity, RACF specifies the scope of the user's authorization for the current terminal session or batch job.

Checking Authorization

After identifying and authenticating the user, RACF controls interaction between the user and the system resources. RACF must authorize:

1. Which users may access resources
2. How the user may access them, such as for reading or for updating

RACF can also authorize *when* a user can access resources, by either time or day.

Figure 5 depicts how RACF uses the RACROUTE REQUEST=AUTH macro to check authorization. The resource managers issue the other RACF macros in a similar manner.

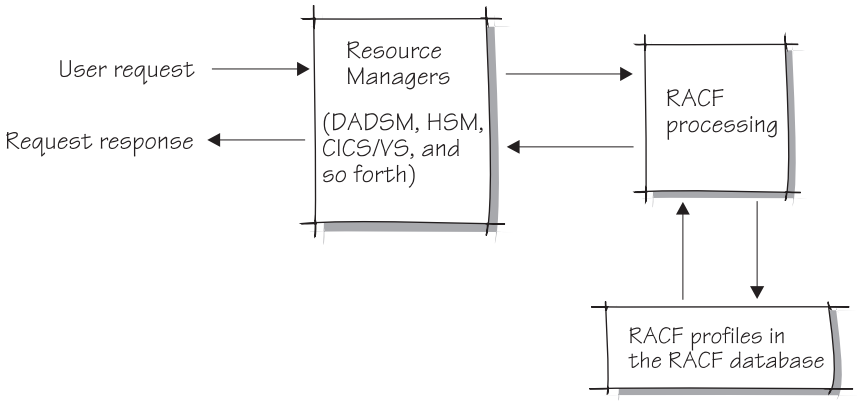


Figure 5. Example of RACROUTE REQUEST=AUTH Processing

Before you can access a resource, RACF:

1. Checks the profiles to determine whether you are authorized to access the resource.
2. Checks the security classification of the user and data.
   a. First, RACF compares the security levels in the user and resource profiles. If the resource has a higher security level than the user, RACF denies the request.
   b. Next, RACF compares the list of categories in your user profile with the list of categories in the resource profile. If the resource profile contains a category that is not in the user's profile, RACF denies the request.
3. Gives you access to the resource if you satisfy any of a number of conditions, such as:
   - The resource is a data set and the high-level qualifier is your user ID.
   - Your user ID is in the access list with sufficient authority.

- Your current connect group is in the access list with sufficient authority.
- The universal access authority (UACC) is sufficiently high.

In Addition:
RACF also provides **global access checking**. This allows you to establish a system-wide in-storage table of default authorization levels for selected resources.

Logging and Reporting

RACF maintains statistical information, such as the date, time, and number of times that a user enters a system and the number of times a specific resource was accessed by any one user. RACF also writes security log records when it detects:

- Unauthorized attempts to enter the system
- Authorized or unauthorized attempts to access RACF-protected resources
- Authorized or unauthorized attempts to enter RACF commands

You can list the contents of these records. You can use them to help you to detect possible security exposures or threats. You can verify the security of the system. Each of the following programs can help you accomplish your goals, depending on your specific needs:

- SMF data unload utility
- RACF report writer
- Data security monitor (DSMON)
- DFSORT ICETOOL

SMF Data Unload Utility

The SMF data unload utility processes SMF records and permits more complex auditing than the RACF report writer.

Output from the SMF data unload utility can be:

- Viewed directly
- Used as input for installation-written programs
- Manipulated by sort/merge utilities
- Uploaded to a database manager, such as DB2

You can process complex inquiries and generate custom-tailored reports from the output of the SMF data unload utility. These reports can be useful in identifying suspicious patterns of access by authorized users that another program might miss. Because data is more often misused by authorized users than stolen by unauthorized users, reports like this are essential to security.

RACF Report Writer

The RACF report writer lists the contents of system management facility (SMF) records in a format that is easy to read. The RACF report writer can also generate reports based on the information in the SMF records, such as:

- Reports that describe attempts to access a particular RACF-protected resource in terms of user identity, number and type of successful accesses, and number and type of attempted security violations
- Reports that describe user and group activity
- Reports that summarize system use and resource use.

The RACF report writer is stabilized at the RACF 1.9.2 level, and is not able to report on many of the later RACF functions.

Data Security Monitor

The RACF data security monitor (DSMON) enables you to verify the basic system integrity and data-security controls. RACF auditors can use the DSMON reports to evaluate the level of security at the installation and to compare the actual level of security at an installation with the planned level of security. As Figure 6 shows, DSMON produces the following reports:

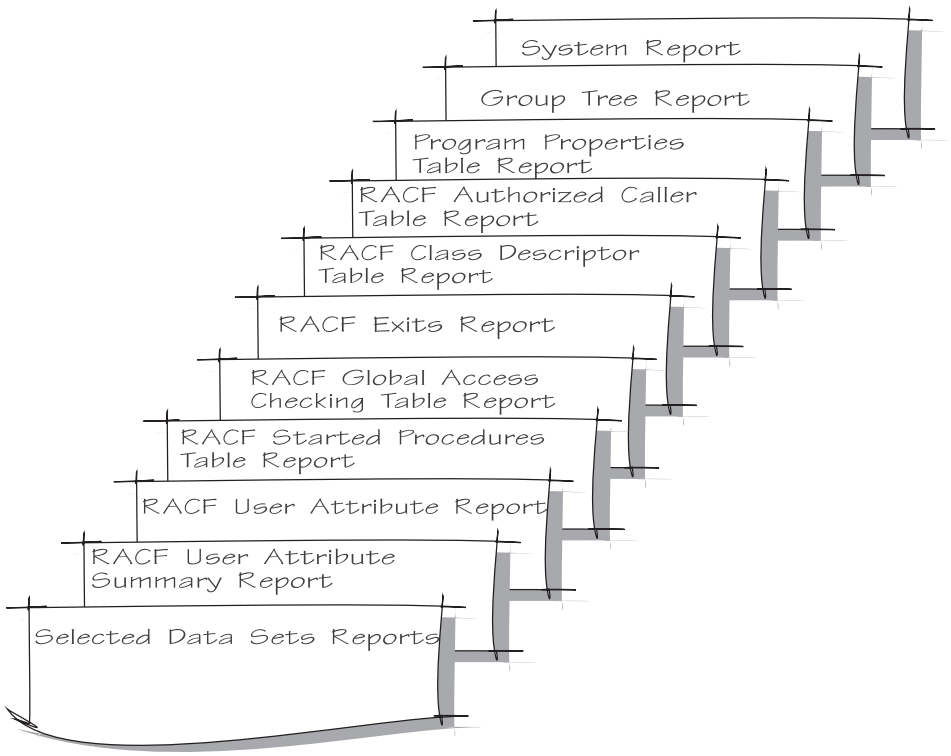


Figure 6. Reports Produced by DSMON

Figure 7 on page 14 illustrates a typical data security monitor report.

```
                                   S E L E C T E D    D A T A    S E T S
                                                VOLUME     SELECTION          R
DATA SET NAME                                   SERIAL     CRITERION          I
-------------------------------------------------------------------------------
GENE.RNR.LOAD                                   D94001     APF                N
LINDAW.RACF22.LOAD                              D94RF1     APF                N
MIKE.WOODST94.LOAD                              D94RF3     APF                N
SIVLE.JAN835.LOAD                               D94RF1     APF                N
DEBBIE.TEST.TOOLS.LOAD                          D94001     APF                N
JOEC.NJ.FRND.LOAD                               D94001     APF                N
                                                           LNKLST - APF
ISPF.ISRLOAD                                    DRV019     APF                N
                                                           LNKLST - APF
LENNON.RTXA.TSO211BW.AUTH.LOAD                  H01TSO     APF                N
SYS1.LINKLIB                                    DRV019     APF                N
                                                           LNKLST - APF
                                                           SYSTEM
SYS1.PARMLIB                                    D94RF1     SYSTEM             N
```

Figure 7. Sample Selected Data Sets Report

DFSORT ICETOOL Utility

RACF uses the DFSORT ICETOOL to produce reports from both SMF data unload and database unload information. The information gathered is used by the RACFICE procedure, which is shipped in the IRRICE member of SYS1.SAMPLIB. As Figure 8 on page 15 and Figure 9 on page 16 show, ICETOOL produces the following reports:

Report	Description
ALDS	Identifies users who alter the access list of the profile
ASOC	Identifies users who can direct commands
BGGR	Finds profiles that aren't protecting what you think they are protecting
CCON	Helps find a performance bottleneck caused by excessive group connections
CGEN	Identifies basic characteristics of the RACF database
CPRO	Identifies basic characteristics of the RACF database
CONN	Identifies users with additional privileges
IDSC	Identifies data set profiles from a conditional access list that allow any authenticated user to access data
IDSS	Identifies data set profiles from a standard access list that allow any authenticated user to access data
IGRC	Identifies general resource profiles from a conditional access list that allow any authenticated user to access data
IGRS	Identifies general resource profiles from a standard access list that allow any authenticated user to access data
OMVS	Identifies users who can use OS/390 UNIX System Services with a non-default UID
SUPU	Identifies users who have superuser (UID(0)) privileges within the OS/390 UNIX System Services environment
UADS	Identifies data set profiles that allow any user to access data
UAGR	Identifies general resource profiles that allow any user to access data
UGLB	Identifies users with extraordinary RACF authority
UGRP	Identifies users with extraordinary group level authority
UIDS	Identifies OS/390 UNIX System Services users who are sharing authority characteristics
URVK	Identifies users who have had a revocation performed
WNDS	Identifies the data set profiles that are in WARNING mode
WNGR	Identifies the general resource profiles that are in WARNING mode

Figure 8. RACFICE Reports Based on the Database Unload Utility (IRRDBU00)

Report	Description
ACD$	Identifies users who are using the RACF remote sharing facility for automatic command direction
CADU	Shows the number of SMF-recorded events.
CCMD	Shows the command activity for a specific user
ECD$	Identifies users who are using the RACF remote sharing facility to explicitly direct commands by specifying “AT(node.user_ID)”
LOGB	Identifies users who are logging on as other users with LOGONBY, a VM facility
LOGF	Identifies users who have exceeded a “bad password” threshold
OPER	Control of users with the OPERATIONS attribute
PWD$	Identifies users who are using password synchronization
RACL	Identifies users who are using the RACF remote sharing facility
RINC	Shows the status of RACF classes at RACF initialization
SELU	Shows all audited events for a user
SPEC	Identifies users with the SPECIAL attribute
TRMF	Identifies intruders who are attempting to guess passwords but are moving from one ID to another to avoid the revocation of user IDs
VIOL	Identifies failed events.
WARN	Identifies events that are allowed but which customers may want to prevent in the future

Figure 9. RACFICE Reports Based on the SMF Data Unload Utility (IRRADU00)

A sample of each of these reports is located in SYS1.SAMPLIB. For a description of the reports created from SMF data unload information, see *OS/390 SecureWay Security Server RACF Auditor’s Guide*. For a description of the reports created from database unload information, see *OS/390 SecureWay Security Server RACF Security Administrator’s Guide*.

Controlling Access to Resources

RACF protects DASD and tape data sets and general resources, such as tape volumes and terminals. RACF controls access to these resources through profiles defined for each resource and user. See “Chapter 3. How You Can Use RACF” on page 25 for more information on the different types of profiles.

When a user requests access to a resource that has a security classification, RACF performs two checks.

1. RACF compares the security level in the user and resource profiles.

   If the resource has a higher security level than the user, RACF denies the request.
2. RACF compares the list of categories in the user’s profile with the list of categories in the resource profile.

These include installation-defined names corresponding to departments or areas within an organization. If the resource profile contains a category that is not in the user's profile, RACF denies the request.

If the security comparison allows access to the RACF-protected resource, you can permit or deny access in either of two ways:

- Explicitly, by assigning each user or group a specific access authority to the resource, or
- Implicitly, with a **universal access authority (UACC)**. All users or groups of users in the system who are not specifically named in a list of authorized users for a resource can still access the resource with the authority specified by the UACC. The UACC also applies to users not defined to RACF.

Remove ID Utility

The remove ID utility helps you eliminate security problems created by old, unneeded user IDs by allowing you to delete residual RACF user IDs and group IDs from the RACF database. This also helps to prevent new users from accessing information they do not need or want. The utility, IRRRID00:

- Uses the output from the database unload utility
- Creates a list of commands to change or remove user IDs and group IDs

In addition, you can remove all the residual IDs at the same time.

How RACF Supports Other Products

RACF provides additional support for interaction with:

IMS/ESA
OS/390 UNIX System Services
OS/390 DCE
OpenEdition for VM/ESA
CICS/ESA
TSO/E
DFSMS
Component Broker for OS/390
DB2
PSF/MVS
APPC/MVS
NetView
Message Queue Manager (MQM/ESA)
CICSplex System Manager (CPSM)
LAN File Service/ESA (LFS/ESA)
Lotus Notes for OS/390
Novell Directory Services (NDS) for OS/390
Tivoli products
SecureWay Security Server Network Authentication and Privacy Service

RACF and IMS/ESA

RACF provides:

- IMS/ESA user verification
- IMS/ESA transaction authorization
- Authorization to IMS/ESA control region resources

If you specify the RACF option during SYSGEN, IMS/ESA calls RACF to build a resident profile for each IMS/ESA transaction defined to RACF, either individually or as a member of a group.

User Verification

RACF user verification is invoked when an IMS/ESA user enters the SIGN ON command. RACF verifies:

- The validity of user identification
- The specified user password

- Authorization to the specified group (if any)
- A new password (if any)
- Authorization to IMS/ESA
- Authorization to the physical terminal
- Date/time verification

Transaction Authorization

Transaction authorization involves checking the in-storage profiles built by RACF to determine if a user or group is authorized to execute the transaction. IMS/ESA invokes RACF transaction authorization checking on each:

- Transaction input from a terminal
- Change call to a modifiable IMS/ESA program control block (PCB)
- /SET command
- /LOCK TRAN command
- /UNLOCK TRAN command
- Insert of a scratchpad area containing a transaction name

If the transaction has not been defined to RACF, IMS/ESA considers the transaction to be unprotected by RACF.

Authorization to IMS/ESA Control Region Resources

IMS/ESA uses RACF to control access to resources that are controlled by the online system. To prevent an unauthorized user from starting a batch message processing (BMP) region and accessing online resources, IMS/ESA specifies the application group name (AGN) to RACF. The AGN name must have been specified in the EXECUTE card parameter list for the BMP if IMS/ESA is using this option.

RACF and OS/390 UNIX

RACF provides security for OS/390 UNIX.

There are three different sets of users who might want to access a file:

- The owner of the file
- The members of the owning group
- All other users on the system

These users might want four different kinds of access permission (of which only three apply to any given file):

- Read
- Write
- Search (directories only)
- Execute (files other than directories only)

OS/390 UNIX protects its data by means of file permission bits. Every file has a three-part string of file permission bits associated with it. The three parts represent the owner, group, and others, and one bit within each part represents each type of access. The owner of the file sets the bits on or off to grant or deny permission to access the file. RACF recognizes these bits and grants or denies access accordingly.

An OS/390 UNIX user with a UID of 0 is a **superuser**. A superuser passes all OS/390 UNIX security checks and can access all OS/390 UNIX resources without restriction. For information on auditing a superuser, see *OS/390 SecureWay Security Server RACF Auditor's Guide*.

Support for OS/390 UNIX helps OS/390 to comply with industry standards that can:

- Make the MVS environment more open
- Lead to increased programmer activity
- Lead to easier application development

With these benefits in mind, OS/390 UNIX supports:

- X/Open Portability Guide Issue 4 (XPG4) base branding functions
- X/Open single UNIX specification
- Network File System (NFS) architecture

XPG4 Base Branding

X/Open Portability Guide Issue 4 (XPG4) allows OS/390 UNIX to port more applications from other systems. It is available and frequently required in the European market.

XPG4 provides Interprocess Communications (IPC) facilities services, which allow two or more distinct processes to share memory, message queues, and so forth. RACF provides authorization checking, permission checking, and auditing for these services to be sure that only authorized processes can communicate with one another.

X/Open Single UNIX Specification

X/Open single UNIX specification provides a common set of application programming interfaces beyond XPG4. It allows both the owner and the superuser to control a file or directory. RACF audits these application programming interfaces.

Network File System (NFS) Architecture

Network file system (NFS) architecture is a set of client/server protocols that allows a client on one machine to access file systems at the server on another machine as if the files were part of the client's local hierarchy. In OS/390 UNIX, NFS architecture allows you to associate a security environment with a particular task.

RACF and OS/390 DCE

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

The interoperation of RACF with DCE enables DCE application servers on MVS to map a DCE user identity (*principal*) to a RACF user ID. This enables DCE application servers that reside on MVS to use the access control and auditing mechanisms provided by RACF in the MVS environment.

It also provides information that OS/390 DCE single signon support uses to log an authenticated OS/390 user into DCE.

By supporting OS/390 DCE, RACF establishes a *cross linking* of identity between a RACF user ID and a DCE principal. This feature allows server applications to use

Understanding RACF Functions

RACF and RACF security services for access control and for auditing the resources that the server applications manage. For more information, see *OS/390 DCE Administration Guide*.

RACF and OpenEdition for VM/ESA

RACF support for OpenEdition for VM/ESA is similar in concept to OS/390 UNIX. If you share a database between VM/ESA and OS/390, you can manage the OpenEdition for VM/ESA data from the OS/390 security server. This centralizes OpenEdition for VM/ESA and OS/390 UNIX user management on OS/390 and allows you to maintain a unique UID for each user across both systems. For more information, see the RACF 1.10 for VM publications.

RACF and CICS/ESA

RACF provides services related to access control for resources used by the Customer Information Control System (CICS), such as CICS/ESA system data sets, program libraries, transactions, regions, files, and databases. These RACF services include:

- User identification and verification
- Resource authorization checking for the CICS/ESA application
- CICS timeout value

In addition, RACF services allow terminal users to manage their own passwords. Using RACF services can simplify the administration of access control and relieve the CICS/ESA system programmer of some of the activities associated with maintaining security-related information in the tables that describe the CICS/ESA resources. For more information, see *CICS RACF Security Guide*.

User Identification and Verification

CICS/ESA invokes the verification service during execution of the sign-on transaction. The verification service:

- Identifies and verifies the user
- Allows the user to change the password
- Requires the user to change the password after it expires
- Revokes access to the system if the user does not provide a correct password in a specified number of attempts

The verification service also checks to see if the user is authorized to access that particular CICS/ESA system and whether the user is authorized to use that terminal.

Resource Authorization Checking

When an application program requests a CICS/ESA resource through the command level interface, CICS/ESA checks to see if the requested resource is RACF-protected. If it is, CICS/ESA asks RACF to determine whether the request is authorized.

- If the user is not authorized, CICS/ESA:
  1. Sends a message to the terminal
  2. Stops the transaction
  3. Logs the violation in the CICS transient data destination
  4. Issues an authorization check request, which causes RACF to write an SMF record and send a message to the security console
- If the user is authorized, CICS/ESA approves the request.

For a list of classes of resources that CICS/ESA protects through RACF, see "Protecting General Resources" on page 30.

CICS/ESA uses a RACF service at system initialization time to bring its resource profiles into main storage. The profiles are brought into main storage to provide maximum performance during security checking.

CICS Timeout Value

CICS/ESA logs off a user who has been inactive for a certain time. This timeout value can be specified in hours and minutes, which allows you to leave an inactive CICS terminal logged on for a maximum is 99 hours and 59 minutes.

RACF and TSO/E

RACF provides TSO/E with user identification and verification, as well as resource authorization checking. To simplify the administration of access control, you can store TSO/E logon information in the RACF database. A segment within the user profile, designated for TSO/E, contains information such as:

JOBCLASS	Default SIZE
MSGCLASS	Default COMMAND
HOLDCLASS	MAXSIZE
SYSOUTCLASS	UNIT
Default ACCTNUM	DEST
Default PROC	USERDATA

When RACF stores this information, TSO/E security administrators need to enter only RACF commands (rather than RACF *and* TSO/E commands) to control their security-related information.

RACF and DFSMS

RACF provides the Data Facility Storage Management Subsystem (DFSMS) with user identification and verification, as well as resource authorization checking. RACF protects:

- VSAM and non-VSAM data sets in integrated catalog facility catalogs
- DFSMS-managed temporary data sets

Advantages:

RACF provides the ability to establish default information on a user or group basis for the DFSMS "constructs" management class and storage class.

- By default, the owner of the data set is the user or group whose RACF ID matches the high-level qualifier of the data set name.
- When it is inappropriate to use the default, RACF allows you to select the owner of the data set.
- RACF supports the VSAM Record Level Sharing (RLS) function of DFSMS/MVS.

In a system-managed storage environment, data sets should *always* be protected with RACF because data set passwords are ignored.

With DFSMS, RACF can protect and control the use of SMS classes, data sets, functions, keywords, and commands.

Understanding RACF Functions

RACF provides the following facilities to support DFSMS:

- General-resource classes in the class descriptor table for use in protecting SMS classes
- A DFP segment in both user and group profiles to contain default information for determining data management and storage characteristics for data sets
- A DFP segment in data set profiles for specifying the owner of SMS-managed data sets protected by the profile
- Field-level access checking to provide security for fields in the DFP segment of user, group, and data set profiles

For more information regarding the protection of DFSMS resources, see *OS/390 SecureWay Security Server RACF Security Administrator's Guide*.

RACF and PSF/MVS

Using RACF with Print Services Facility/MVS (PSF) Release 3 or later, and with the appropriate RACF classes active, separator pages can be created at the beginning and end of jobs. These pages cannot be falsified or suppressed by the user. In addition, information associated with the security label of the data can be printed on each page of output.

RACF and APPC/MVS

RACF support for Advanced Program-to-Program Communication (APPC/MVS) provides a security environment and audit capabilities for APPC transactions. RACF manages APPC lists of users who have signed on to one system and communicate with another through APPC (signed-on-from lists). In addition, with RACF's support for network–qualified names, logical units (LUs) do not have to be renamed when networks that contain MVS systems are added to your installation.

RACF and NetView

RACF provides security for NetView. It uses NetView classes and the NETVIEW segment in the user profile to check the authority of network commands and to check the authority of NetView operators to start spans.

RACF and MQM/ESA

Message Queue Manager (MQM/ESA) is a product implementing SAA Message Queuing for MVS/ESA. RACF provides command checking and holds information for administrative functions. It also provides security for the queue, process, and namelist resources.

RACF and Component Broker for OS/390

RACF support for Component Broker for OS/390 enables a user's security environment to be easily retrieved and transported to another address space. Component Broker for OS/390 provides an object request broker that allows application programs to locate objects that are distributed throughout the network. With the support provided in RACF, these object-oriented applications can use the security advantages provided in OS/390.

RACF and DB2

The OS/390 Security Server provides source code, the RACF/DB2 external security module in SYS1.SAMPLIB, that you can assemble and linkedit into DB2. This routine serves as a common security point that allows profiles in the RACF database to control access to DB2 resources. RACF protection allows you to:

- Administer and audit access control from a single point of control
- Define security rules before a DB2 object is created
- Maintain security rules when a DB2 object is dropped
- Control access to DB2 objects with generic profiles
- Control access to DB2 objects for single or multiple subsystems with a single set of RACF profiles
- Validate a user ID before permitting it access to a DB2 object

CICSPlex System Manager Support

RACF provides security for CICSPlex System Manager (CPSM) by protecting both the access to and the use of the system management functions. RACF also controls the simulation of CICS command checking and CICS resource checking.

LAN File Service/ESA Support

RACF provides security for LAN File Service/ESA (LFS/ESA). If LAN File Service/ESA is installed, you can use the RACF LFSCLASS to control access to workstation data stored on the host. For information on using the LFSCLASS, see *OS/390 SecureWay Security Server RACF Security Administrator's Guide*.

RACF and Tivoli Products

RACF provides programming interfaces that enable the Tivoli User Administration and Tivoli Security Management products to manage profile data on the RACF database. A RACF command line is also provided on the Tivoli desktop.

RACF and Lotus Notes for OS/390

The interoperation of RACF with Lotus Notes for OS/390 enables it to map a Lotus Notes identity to a RACF user ID and to map a RACF user ID to a Lotus Notes identity. This enables Lotus Notes for OS/390 to use the access control and auditing mechanisms provided by RACF.

RACF and NDS for OS/390

The interoperation of RACF with NDS for OS/390 enables NDS for OS/390 to map an NDS identity to a RACF user ID and to map a RACF user ID to an NDS identity. This enables NDS for OS/390 to use the access control and auditing mechanisms provided by RACF.

RACF and SecureWay Security Server Network Authentication and Privacy Service

Network Authentication and Privacy Service uses RACF to store and administer information about realms and principals, using RACF user profiles and general resource profiles. The user profile stores information about Network Authentication and Privacy Service user principals on your local system. The general resource classes allow you to map principals to the RACF user IDs on your system and to define a local Network Authentication and Privacy Service realm and its trust relationships with foreigh realms.

By incorporating the Network Authentication and Privacy Service registry into the RACF registry, you have no need for a separate registry of security information on OS/390.

For information regarding this function, see *OS/390 SecureWay Security Server RACF Security Administrator's Guide*.

Chapter 3. How You Can Use RACF

Data security is *the protection of data from accidental or deliberate unauthorized disclosure, modification, or destruction*. Based on this definition, it is apparent that all data-processing installations have at least potential security or control problems. Users have found, from past experience, that data security measures can have a significant impact on operations in terms of both administrative tasks and demands made on the end user. This chapter provides some suggestions that might be useful in understanding who will use RACF and how to use it in the most effective way.

RACF gives the user defined with the SPECIAL attribute—the security administrator—many responsibilities both at the system level and at the group level. As the security administrator, you are the focal point for planning security at your installation. You need to:

- Determine which RACF functions to use
- Identify the level of RACF protection
- Identify which data RACF is to protect
- Identify administrative structures

Determining the RACF Functions to Use

RACF provides many functions to help achieve the level of protection needed for your installation. Some of the factors that determine what functions to select are:

- Your security objectives
- The security measures that already exist
- An evaluation of how RACF can help you reach your goals

If you require security for part or all of your installation's database, you can use RACF to define and protect these parts. If you want to limit the users who can access certain data, and make RACF "invisible" to some users, you can define these restrictions with user attributes, group structures, and access authorities within group structures. RACF provides a very flexible approach for defining which users can use which data.

The key factor is to understand what RACF functions you want to use in order to achieve your security goals. The following list shows some RACF functions that you might use and relates these functions to the security they provide.

RACF Function
Security Provided

Data Set Protection
You can protect:
- DASD and tape data sets
- New and existing data sets

Protection can be gradually phased in.

Resource Protection
You can protect several classes of resources, such as load modules, terminals, applications, tape volumes, and user-defined resources. Protection can be gradually phased in.

Naming Conventions
You can use your own data set naming conventions. RACF provides a table

to help you do this easily. Because implementing RACF security is easier when your installation already has a consistent data set naming convention, you can use the installation of RACF as an opportunity to implement consistent naming conventions.

Organization
You can define RACF groups to map the existing organizational structure. RACF provides flexibility of control and administration, allowing various degrees of central control and delegated control.

Group Names
RACF provides for group structures and user IDs. You can base the groups on the user functions performed if you want.

Transparency
You can use discrete profile modeling and generic profiles to provide for end-user transparency and transparent protection for data sets.

RACF Tailoring
You can use installation exits for customizing RACF processing.

Recovery
RACF provides a controlled environment during recovery of the RACF database.

Violation Detection
You can use RACF's logging, reporting, and auditing capabilities to detect violations.

Subsystems
You can control the use of IMS/ESA and CICS/ESA resources.

Networks
You can decide whether to trust information received from submitting nodes.

Data Sharing
You can choose whether to place database records in

- A central buffer shared by every system in a sysplex
- Each system's individual buffer, reducing I/O to the database on DASD

Data sharing also allows you to use the coupling facility to add a level of buffers for the RACF database in addition to the in-storage buffers that already exist. This further reduces the need for DASD I/O to read from the RACF database.

Performance Considerations

RACF's effect on system usage depends on the type and number of RACF functions performed and the I/O activity to the RACF database.

Reducing and Balancing I/O Activity

RACF provides options to reduce and balance I/O activity:

- By using resident data blocks, you can reduce the number of I/O requests to the RACF database. This option is strongly recommended.
- By using the multiple RACF database option, you can split the RACF database into many RACF databases across a number of devices. This can:
  - Balance I/O activity by spreading the accesses across devices, thus reducing the possibility of device contention.
  - Reduce the number of resources made unavailable by the loss of one database or device.

- By using the RACF remote sharing facility, you can share a database with other systems, each system using its own copy of that database.

Improving System Performance

RACF provides other options that may, under certain conditions, improve system performance.

Option	Benefit
• Generic profile checking	• Reduces the frequency of I/O requests
• Global access checking	• Allows you to use an in-storage table instead of normal profile processing
• RACF statistics options	• Reduces I/O activity
• RACF logging options	• Reduces I/O activity
• Hiperbatch processing	• Reduces I/O to the RACF database and can reduce processing time
• SETROPTS RACLIST processing for a class	• Improves processing time for certain groups of users
• Group tree in storage processing	• Uses the coupling facility's central buffer to reduce I/O

You can take advantage of the MVS/ESA Virtual Lookaside Facility (VLF) to reduce RACF database I/O during group authority processing and to store accessor environment elements (ACEEs) in data spaces.

The RACF Database

The Security Server (RACF) database uses a blocksize of 4096 for all records.

Identifying the Level of Resource Protection

RACF allows you to specify different levels of protection for your resources and to gradually increase the level of RACF protection. In all cases, you can use RACF to report about access to the resources. You can:

- Allow or deny access to resources, and log and report user access to resources.
- Issue and log warning messages about user access to resources that would normally be denied, but allow access for a limited time. This is called the **grace period.** You can use the grace period to begin RACF protection without denying access until a later date.
- Provide full RACF protection to your resources and log and report both successful and unsuccessful access attempts.

Government Security Levels

The United States Department of Defense (DoD) has established security criteria for its computer systems and for those systems that perform government work under contract. Each system is evaluated and awarded a security rating, depending on the extent the system protects resources and its own processing. These ratings are, in ascending order of security, D, C1, C2, B1, B2, B3, and A1. OS/390 has not been evaluated for certification.

Identifying the Data to Protect

Every installation has varying amounts of confidential data and varying degrees of confidentiality. However, more and more installations are choosing to protect most, if not all, of their resources. What you should consider is how to protect resources in a simple yet effective manner and how to achieve this protection with minimum impact on the end user.

The task of protecting large quantities of data can take on significant proportions unless you can acquire protection automatically. In the case of new data, it is simple and, once the controls are in place, practically free from administrative overhead.

Resource Profiles

RACF maintains information entries called **profiles** in the RACF database. It uses them to protect DASD and tape data sets and general resources, such as tape volumes and terminals.

- **Data set profiles** contain security information about DASD and tape data sets.
- **General resource profiles** contain security information about general resources.

Each RACF-defined resource has a profile, though you can optionally use a single profile to protect multiple resources. Figure 10 illustrates a general resource profile. A data set profile is very similar.

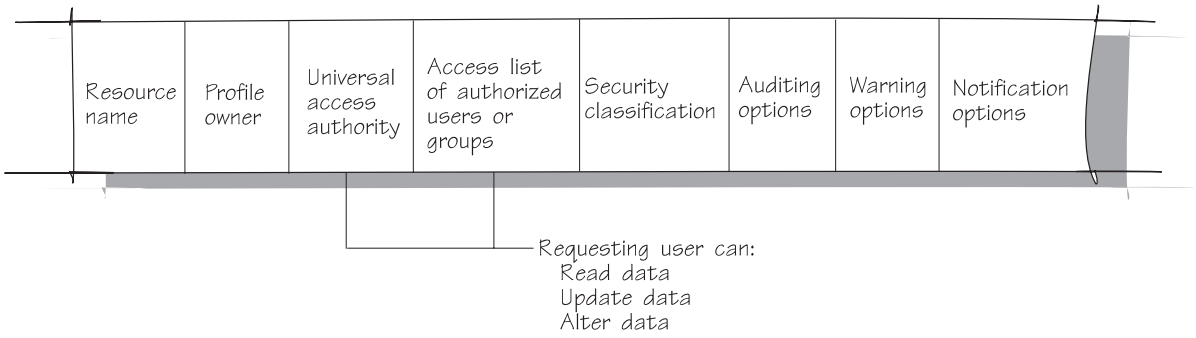


Figure 10. Key Fields in a General Resource Profile

Types of RACF Profiles

RACF provides discrete, generic, and grouped resource profiles for both data sets and general resources.

- **Discrete profile**

  Discrete profiles have a one-for-one relationship with a resource—one profile for each resource. Discrete profiles provide very specific levels of control and should be used for sensitive resources. They protect only the one identified data set that is on the specified volume or that spans specific volumes. For example, a single data set can be defined with a discrete profile to allow access by one user.

- **Generic profile**

  Generic profiles have a one-for-many relationship. One profile controls access to one or more resources whose names contain patterns or character strings that RACF uses to associate them with each other. They contain a list of the authorized users and the access authority of each user. A single generic profile

can protect many data sets that have a similar naming structure. For example, all data sets that have a high-level qualifier of JONES and the characters SIVLE1 as a second-level qualifier can be controlled with one generic profile.

Advantages of Generic Profiles:

- The administrative effort is reduced in controlling access to a large number of resources that have similar names and the same access list. Data sets protected by generic profiles do not have to be defined individually to RACF. This can result in a smaller RACF database and a savings in time and maintenance.
- If used properly, generic profiles can result in better performance because of reduced I/O activity. When you load generic profiles into main storage, they remain there as long as possible.

- **Grouped profile**

  Another type of RACF profile is the grouped profile. There may be no way to associate the resources with a common access list based on patterns in the resource names. In this case, the many resource names can be associated with a single RACF profile through the use of a grouping profile that contains the names of the associated resources.

  Some subsystems with high performance requirements, such as IMS/ESA, have the profiles resident in the subsystem address space. These subsystems can save main storage by using grouped profiles.

Profile Modeling

You can use profile modeling to copy information (such as the access list, owner, logging options, and so forth) from an existing profile when defining a new profile. This greatly reduces the effort needed to create new profiles.

You can establish profile modeling with either of the following:

- A RACROUTE REQUEST=DEFINE preprocessing installation exit routine
- The SETROPTS command

RACF also allows you to specify an existing profile name that RACF uses as a model when creating the new profile.

Protecting Data Sets

To protect a data set, RACF builds a data set profile and stores it in the RACF database. You can protect tape data sets and the following types of DASD data sets:

- Cataloged and uncataloged non-VSAM data sets
- VSAM data sets
- Data sets that have the same name but reside on different volumes
- Generation data group (GDG) data sets
- Data sets and catalogs with single-level names obtained through an installation-supplied prefix
- Controlled programs used with OS/390 UNIX

Advantages of RACF Protection:

- Only authorized users can access the data set. With password protection, any user who knows the password can access the data set.
- You can run jobs more easily with RACF protection because the system does not prompt the operator for data set passwords for RACF-protected data sets accessed during a job.

RACF can also protect data sets that are password-protected. If the data set is password-protected, you must supply the password when creating a discrete profile. When a password-protected data set is also RACF-protected, access to the data set is determined only by RACF processing; password processing is bypassed. You can write an exit routine to modify RACF, however, so passwords can be used with RACF at your installation.

Tape Data Set Restrictions:

- Tape data set protection is not in effect when you install RACF. You must issue the SETROPTS command with the TAPEDSN option, as well as activate the TAPEVOL general resource class, to activate tape data set protection.
- Tape data set protection is available only on systems that have Data Facility Product Version 2 Release 1 or later installed.

New Data Sets

RACF provides several ways to protect new data sets:

- When generic profile checking is active, RACF protects new data sets automatically if the data set name matches an existing generic profile name.
- You can automatically RACF-protect data sets by:
  - Assigning the ADSP attribute to the user
  - Using the PROTECT or SECMODEL operands on the JCL data definition or TSO ALLOCATE statements for the data set.

  You can also combine profile modeling with this process.
- You can protect (but not automatically) any new data set with the RACF ADDSD command (or the DATA SET series of panels). To enforce RACF-protection of new data sets, see the SETROPTS command in *OS/390 SecureWay Security Server RACF Command Language Reference*.

Protecting General Resources

Just as you can protect a DASD or tape data set, you can define the **general resources** you want to protect with RACF. These include:

Volumes: • DASD • Tape	Load modules (programs)
IMS/ESA: • Transactions • Transaction groups • Application groups	TSO: • Logon procedures • Account numbers • User attributes • Performance groups

Vector Facility	Operations Planning and Control/Advanced (OPC/A)
CICS/ESA: • Transactions • Started transactions • Scheduled program specification blocks (PSBs) • Files • Journals • Programs and programmer commands • Transient data destinations • Temporary storage definitions	DFSMS: • Management class • Storage class
Applications: • MQM/ESA • NetView • DATABASE 2	Terminals
Installation-defined resources	

RACF builds a **general resource profile**. Like profiles for data sets, general resource profiles can be generic or discrete.

Defining Resource Classes, Groups, and Members

RACF recognizes **resource classes** as those resources that are similar to each other. A tape volume, regardless of its contents or physical location, represents, for example, a specific way of storing data; tape volumes are a resource class. As another example, terminals might have different physical attributes, but they all perform similar input/output functions; terminals are a resource class.

When you define a resource class, RACF places control information for the new resource class into a **class descriptor table**. The control information includes:

- The resource class name
- The syntax rules for the resource names within the class
- The location of the auditing and statistics flags for the class

You must supply the necessary control information for any new classes you define. RACF supplies the control information for the predefined resource classes.

When defining a new resource class, you can optionally designate that class as either a resource **group** class or a resource **member** class. For a resource group class, any user or group of users permitted access through a profile for that resource group is permitted access to all members of that profile.

RACF uses the class descriptor tables whenever it makes a class-related decision (such as, “Should auditing be done for this class?”). The class descriptor tables and the appropriate use of RACF authorization-checking services can extend RACF protection to any part of the system.

Protecting Installation-Defined Resource Classes

For most resources managed by IBM systems, subsystems, and applications, calls to RACF are handled internally and there is nothing you need to do about them. However, RACF is very flexible and is designed so you can call RACF directly if you wish. To use RACF services directly, do so through RACF macros. For more information about the macros and the services they provide, see *OS/390 SecureWay Security Server External Security Interface (RACROUTE) Macro Reference*.

Protection with RACF Disabled (Failsoft Protection)

RACF, even when partially disabled in a system, provides some protection and offers default services. RACF can use various internal tables to verify requests for protected resources, can route control to various exit routines for further processing, and can log the requests, whether they are granted or denied.

Identifying Administrative Structures

Your organization's data-access patterns are probably well established by department or function or both. You can regard each department or function as a group and define these groups to RACF. Groups are the key element in your RACF scheme, and the underlying security requirement tends to be for group isolation. You can make group isolation automatic and transparent to end users. Group isolation is easy to implement and gives a wide base on which to refine your security controls. A RACF group also serves as a focal point for delegating authority to users within the group and for controlling the data sets associated with the group.

Identifying Your User and Group Relationships

Identifying and defining user and group relationships make it simpler and more efficient to protect resources that those users and groups create, share, or use. In instances where some groups require exceptional access controls, you might subdivide your organization to minimize occasions when data needs to be passed between these groups and the rest of the organization. If the users in a group share common access requirements, as is often the case, the administrative task of authorizing users is greatly simplified.

In many cases, it might be enough to simply isolate development work from production. On the other hand, it might be practical to isolate many individual users and groups. In either case, you must arrange the groups in a structure to form a hierarchical tree so that each RACF group (except the highest) is a subgroup of another group. The RACF-supplied group SYS1 must be the highest group in the structure. The relationship between superior groups and subgroups is administrative and does not necessarily imply any authorization to resources.

Identifying Your Users

Before you can implement RACF, you need to understand the responsibilities of the various users during the planning stages and installation of RACF. The following list shows typical user responsibilities.

User Responsibility

Security Administrator
The security administrator has the overall responsibility for RACF implementation. The security administrator reviews and approves all implementation phases, selects the resources to be protected, and plans the order in which protection will be implemented. In addition, the security administrator should be responsible (or should delegate the responsibility to group administrators) for educating the installation users about how RACF will be implemented. (That is, will there be a grace period before the new security procedures take effect? Or, how will the implementation of RACF affect the day-to-day responsibilities of each user?)

Group Administrator
During planning, the group administrators are user representatives who represent major application areas.

Other Administrators

If appropriate, other users (for example, a helpdesk administrator, a TSO/E administrator, or a database administrator) might be considered as members of the implementation team. A database administrator might be selected to represent protection for the DB/DC environment, including:

- DB/DC users
- Accessibility to DB/DC subsystems
- Terminal and transaction protection
- Database protection for batch access

Auditor

The auditor provides guidance on good auditing practices related to data security and user access. The auditor determines and selects the necessary RACF logging and reporting options to provide an effective audit of security measures.

Technical Support

The system programmer who provides technical support for RACF installs RACF in the system and maintains the RACF database. This person has overall responsibility for the programming aspects of system protection and provides technical input on the feasibility of various aspects of the implementation plan. In addition, the technical-support person writes, installs, and tests RACF exit routines. Note that, although there is no "technical support" attribute, this person has an important role in implementing RACF. The technical-support person might very well be assigned the RACF OPERATIONS attribute.

Operator

The user with the OPERATIONS attribute has authority to perform certain "housekeeping" operations on RACF-protected resources (for example, dump/restore).

End User

The end user is the person who is using the RACF-protected system. The end user logs onto the system and accesses the resources on the system.

Defining Users

RACF allows you to define the users who can access the protected resources. It records information about the users in the **user profiles**, and maintains this information in the **RACF database** (along with all other profiles).

Figure 11 on page 34 illustrates a user profile. Each RACF-defined user has a user profile.

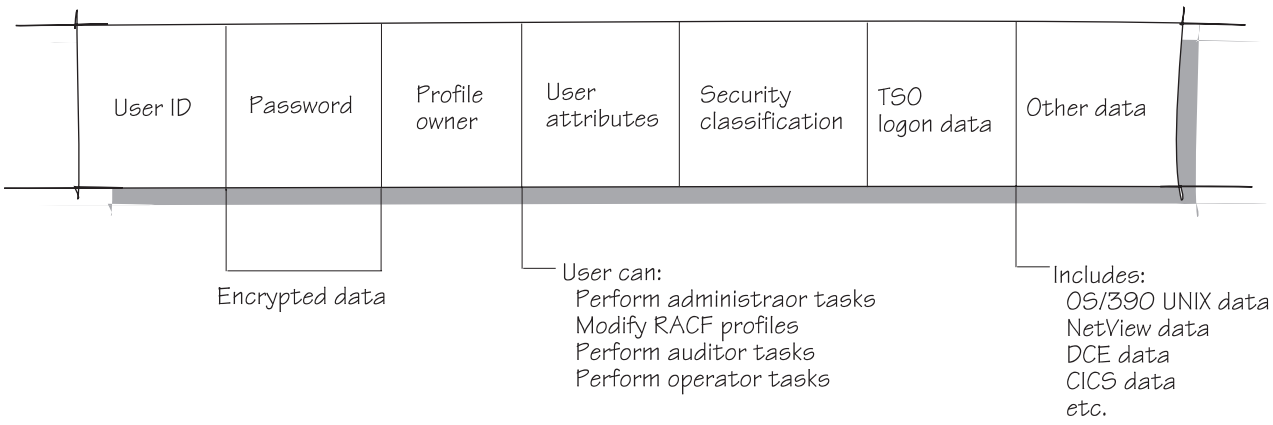


Figure 11. Key Fields in the User Profile

The **user attributes** define the responsibilities, authorities, or restrictions that a specific user has while defined to the system. The **security classification** determines the user's ability to access sensitive resources.

The user data that describes an OS/390 UNIX user includes a **user identifier** (UID), which is a numeric value between 0 and 2147483647. This takes the place of the user ID. When you try to access a sensitive resource, RACF determines whether you have an adequate security classification for that resource.

Defining Groups

With RACF, all defined users belong to at least one group, known as a default group. A **group** is a collection of RACF users who share common access requirements to protected resources or who have similar attributes within the system. In OS/390 UNIX, groups are defined by a **group identifier** (GID).

Groups associate similar jobs or projects together for administrative convenience. You can think of the groups as forming a hierarchical or "tree" structure, where each group is "owned" by a superior group. Groups can also "own" resources, as well as users and other groups. Figure 12 illustrates this.

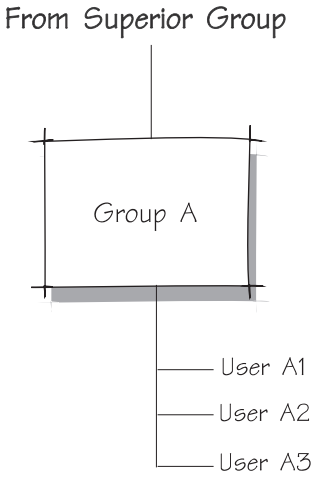


Figure 12. RACF Users Associated with a Group

RACF records information about the groups in the **group profile**, which reside in the RACF database.

Connecting Users to Groups

As a RACF user, you can be a member of more than one group. In RACF terminology, you are **connected** to that group.

A group owner—usually the user who defined the group to RACF—can define and control the other users connected to the group. The group owner can also delegate various group administrative responsibilities and authorities to other users connected to the group. The **connect information** in your user profile describes what you can do when connected to that group, and includes your **group authorities** and **group-related user attributes**, as well as other information.

Figure 13 illustrates, in the non-shaded area, how a user with a group-related user attribute in Group A can affect the resources or profiles associated within Group A and its subgroups, Group A1 and Group A2. This user cannot affect resources or profiles associated with Group B.

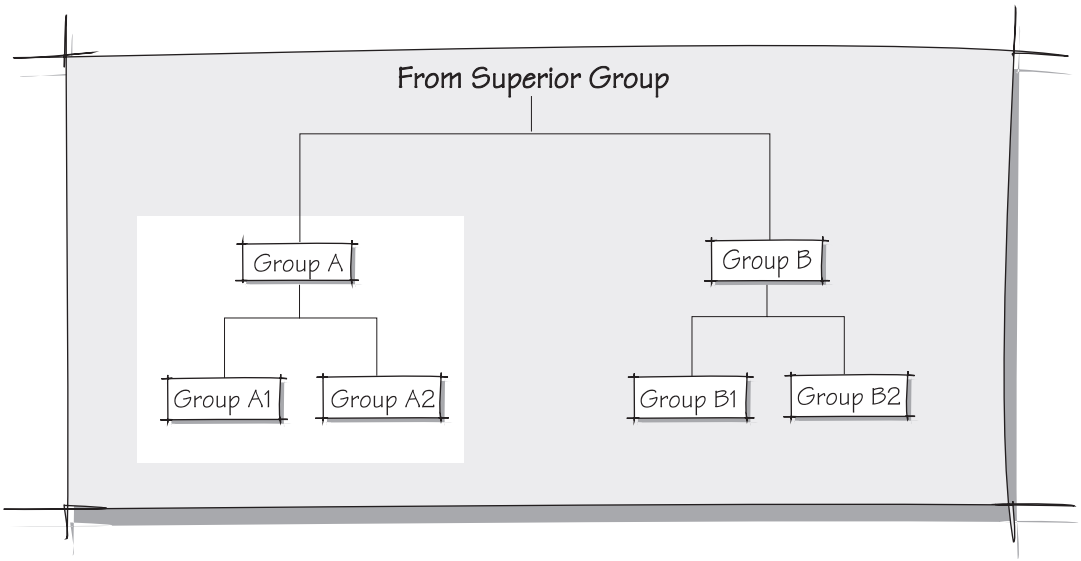


Figure 13. RACF Group-Related Attribute Control

Appendix. Notices

This information was developed for products and services offered in the USA. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

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

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA

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

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

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

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

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs

and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Mail Station P300
2455 South Road
Poughkeepsie, NY 12601-5400
USA

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

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

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

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

This product contains code licensed from RSA Data Security Incorporated.

Trademarks

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

AIX/6000	IBM	Print Services Facility
BookManager	IBMLink	PSF
CICS	IMS/ESA	RACF
CICS/ESA	Library Reader	S/390
CICSPlex	MVS/ESA	SAA
DATABASE 2	NetView	SecureWay
DB2	OPC	System/390
DFSMS	OpenEdition	TalkLink
DFSMS/MVS	OS/2	VM/ESA
Hiperbatch	OS/390	VTAM

Lotus and WebSphere are trademarks of Lotus Development Corporation in the United States, or other countries, or both.

Tivoli is a trademark of Tivoli Systems, Inc. in the United States, or other countries, or both.

Windows is a trademark of Microsoft Corporation.

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

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

Index

I

L

M

N

O

P

R

S

T

U

V

X

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

OS/390
SecureWay Security Server RACF Introduction

Publication No. GC28-1912-07

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

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

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

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

Please tell us how we can improve this book:

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

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

Name _____ Address _____

Company or Organization _____

Phone No. _____

Readers' Comments — We'd Like to Hear from You
GC28-1912-07

IBM

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
2455 South Road
Poughkeepsie, NY
12601-5400

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

GC28-1912-07

Cut or Fold
Along Line

Program Number: 5647-A01

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

GC28-1912-07