

z/OS



Security Server RACF General User's Guide

z/OS



Security Server RACF General User's Guide

Note

Before using this information and the product it supports, be sure to read the general information under "Notices" on page 103.

Sixth Edition, September 2009

This is a major revision of SA22-7685-04. This edition applies to Version 1 Release 11 of z/OS (5694-A01), and to all subsequent releases and modifications until otherwise indicated in new editions.

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

International Business Machines Corporation
MHVRCFS, Mail Station P181
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)

Internet e-mail: mhvrcfs@us.ibm.com

World Wide Web: <http://www.ibm.com/systems/z/os/zos/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 document
- 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.

© Copyright International Business Machines Corporation 1994, 2009.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Tables	vii
Figures	ix
About this document	xi
Who should use this document	xi
What you should know before reading this document	xi
How to use this document	xi
Where to find more information	xi
Softcopy documents	xii
RACF courses	xii
IBM systems center publications	xiii
Other sources of information	xiii
IBM discussion areas	xiii
Internet sources	xiii
The z/OS Basic Skills Information Center	xiv
To request copies of IBM publications	xv
Summary of changes	xvii
Chapter 1. What is RACF?	1
Identifying and verifying users	1
Authorizing users to access protected resources	2
Recording and reporting access attempts	3
Chapter 2. Using RACF panels	5
Chapter 3. Using RACF commands	7
RACF commands for general user tasks	7
Getting online help for RACF commands	10
Escaping from a command prompt sequence	10
Using command abbreviations	10
Directing commands	10
Automatic command direction	12
Getting help for RACF messages	12
Viewing notification messages	13
Chapter 4. How am I defined to RACF?	15
Finding out if you are defined to RACF	15
Finding out how you are defined to RACF	16
Understanding the information RACF has about you as a user	17
Finding out what authority you have as a member of a group	20
Examples of output of the LISTUSER command	23
Finding out what CICS information RACF has about you	24
Finding out what custom field information RACF has about you	25
Finding out what DCE information RACF has about you	26
Finding out what distributed identity information RACF has about you	27
Finding out what DFSMSdfp information RACF has about you	28
Finding out what EIM information RACF has about you	28
Finding out what Kerberos information RACF has about you	29
Finding out what language information RACF has about you	30
Finding out what Lotus Notes information RACF has about you	31
Finding out what NetView information RACF has about you	31

Finding out what OpenExtensions information RACF has about you	33
Finding out what OPERPARM information RACF has about you	33
Finding out what z/OS UNIX information RACF has about you	35
Finding out what TSO/E information RACF has about you	37
Finding out what WORKATTR information RACF has about you	38
Finding out if your password is synchronized with other IDs	39
Finding out what user ID associations are defined for you	39
Automatic registration of digital certificates	41
Listing your digital certificate information	41
Chapter 5. Changing how you are defined to RACF	43
Changing your password	43
Changing your password phrase	44
Synchronizing your passwords and password phrases	45
Automatic password direction	46
Logging on to TSO/E with a group other than your default group	47
Logging on with a security label other than your default security label	48
Allowing another user to submit your jobs	50
User ID associations	51
Defining a peer user ID association with password synchronization	52
Defining a peer user ID association without password synchronization	52
Defining a managed user ID association	53
Approving user ID associations	53
Deleting user ID associations	54
Chapter 6. Protecting a data set	55
Choosing between discrete and generic profiles	55
Creating a discrete profile to protect a data set	57
Creating a generic profile to protect a data set	59
Finding out how a data set is protected	64
Finding out what data set profiles you have	69
Deleting a data set profile	69
Chapter 7. Protecting data on tapes	71
Chapter 8. Changing access to a data set	73
Changing the universal access authority to a data set	73
Permitting an individual or a group to use a data set	74
Using ID(*) in an access list	75
Denying an individual or a group use of a data set	75
Including the individual or group on the access list with ACCESS(NONE)	76
Removing the user or group from the access list	76
Chapter 9. Protecting general resources	79
Searching for general resource profile names	79
Listing the contents of general resource profiles	80
Permitting an individual or a group to use a general resource	81
Denying an individual or a group use of a general resource	82
Including the individual or group on the access list with ACCESS(NONE)	82
Removing the individual or group from the access list	83
Appendix A. Reference summary	85
Access authority for data sets	85
Access authority for general resources	86
Profile names for data sets	86
Generic profile rules when enhanced generic naming is inactive	86

Generic profile rules when enhanced generic naming is active	88
When data set profile changes take effect	89
Automatic direction of application updates	90
Supplied RACF resource classes	91
Supplied resource classes for z/OS systems	91
Supplied resource classes for z/VM systems	99
Appendix B. Accessibility	101
Using assistive technologies	101
Keyboard navigation of the user interface.	101
z/OS information	101
Notices	103
Policy for unsupported hardware	104
Trademarks.	105
Index	107

Tables

1.	RACF command table for general user tasks	7
2.	Generic naming for data sets with enhanced generic naming inactive: * at the end	87
3.	Generic naming for data sets with enhanced generic naming inactive: * in the middle or %	87
4.	Generic data set profile names created with enhanced generic naming active: * and **	88
5.	Generic data set profile names created with enhanced generic naming active: *, **, or % in the middle.	89
6.	Resource classes for z/OS systems	91
7.	Resource classes for z/VM systems	99

Figures

1.	The RACF primary menu panel	5
2.	A directed LISTGRP command: sample output	11
3.	A directed ADDSD command: sample output	11
4.	An automatically-directed ADDUSER command: sample output	12
5.	An automatically-directed RDEFINE command: sample output	12
6.	A sample logon panel	15
7.	LISTUSER output: description	17
8.	LISTUSER output: example 1	23
9.	LISTUSER output: example 2	24
10.	LISTUSER output: description of the CICS information	25
11.	LISTUSER output: sample CICS information.	25
12.	LISTUSER output: sample custom field information	26
13.	LISTUSER output: description of the DCE information	26
14.	LISTUSER output: sample DCE information	27
15.	Sample RACMAP output	27
16.	LISTUSER output: description of the DFSMSdfp information	28
17.	LISTUSER output: sample DFSMSdfp information	28
18.	LISTUSER output: description of the EIM information	29
19.	LISTUSER output: sample EIM information	29
20.	LISTUSER output: description of the Kerberos information	30
21.	LISTUSER output: sample Kerberos information	30
22.	LISTUSER output: description of the language information	30
23.	LISTUSER output: sample language information	31
24.	LISTUSER output: description of the information related to Lotus Notes	31
25.	LISTUSER output: sample Lotus Notes information	31
26.	LISTUSER output: description of the NetView information	32
27.	LISTUSER output: sample NetView information	32
28.	LISTUSER output: description of the OpenExtensions information	33
29.	LISTUSER output: OpenExtensions information (example 1)	33
30.	LISTUSER output: OpenExtensions information (example 2)	33
31.	LISTUSER output: description of the OPERPARM information	34
32.	LISTUSER output: sample OPERPARM information	35
33.	LISTUSER output: description of the z/OS UNIX information	36
34.	LISTUSER output: z/OS UNIX information (example 1)	37
35.	LISTUSER output: z/OS UNIX information (example 2)	37
36.	LISTUSER output: description of the TSO/E information	38
37.	LISTUSER output: sample TSO/E information	38
38.	LISTUSER output: description of the WORKATTR information	39
39.	LISTUSER output: sample WORKATTR information	39
40.	RACLINK LIST output: user ID association information (example 1)	40
41.	RACLINK LIST output: user ID association information (example 2)	40
42.	RACLINK LIST output: user ID association information (example 3)	41
43.	Example: listing your digital certificate information.	41
44.	Listing your digital key ring information	42
45.	Automatic password direction: sample output	47
46.	Logging on to another group	48
47.	Logging on with another security label	50
48.	LISTDSD command: sample output	65
49.	A successful application update: sample output	90
50.	When the user ID is revoked: sample output.	91

About this document

This document contains information about the Resource Access Control Facility (RACF®), which is part of the Security Server for z/OS®.

This document teaches the general user how to use RACF to perform security functions. It contains an introduction to RACF, as well as sections that guide the user through basic security tasks.

Who should use this document

This document is for general users who need to use RACF to protect their own data sets or general resources, and for users responsible for the security of group data sets. You can use either panels or commands to perform these tasks. This document also explains how to authorize another user to submit jobs for you.

What you should know before reading this document

This document assumes that you know how to conduct a terminal session on your system. For more information about a TSO/E terminal session, see *z/OS TSO/E Primer*.

To use RACF, you must:

- Know how to conduct a TSO/E terminal session
- Know how to enter commands or use ISPF panels
- Be defined to RACF

How to use this document

To use this document:

- Read Chapter 1, “What is RACF?,” on page 1. It tells you how RACF provides security on the operating system and protects your resources.
- Choose whether to use the RACF panels or commands to perform the security tasks.
 - If you want to use panels, read Chapter 2, “Using RACF panels,” on page 5. This chapter explains how to get help while using the RACF panels.
 - If you want to use commands, Chapter 3, “Using RACF commands,” on page 7 contains a table of commands to help you perform your security tasks.
- Read Chapter 4, “How am I defined to RACF?,” on page 15 through Chapter 9, “Protecting general resources,” on page 79. These chapters contain step-by-step procedures for you to follow; they do not require that you have had any previous experience with RACF.
- Use Appendix A, “Reference summary,” on page 85 as a reference for information such as access authority, naming conventions, and RACF-defined classes.

Where to find more information

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

Softcopy documents

The RACF library is available on the following CD-ROM, DVD, and online library collections, in both BookManager® and Portable Document Format (PDF) files. The collections include Softcopy Reader, which is a program that enables you to view the BookManager files. You can view or print the PDF files with an Adobe® Reader.

SK3T-4269 *z/OS Version 1 Release 11 Collection*

This collection contains the documents for z/OS Version 1 Release 11, on CD-ROM discs.

SK3T-4271 *z/OS Version 1 Release 11 and Software Products DVD Collection*

This collection contains the documents for z/OS Version 1 Release 11 and the libraries for multiple releases of more than 400 z/OS-related software products, on two DVDs.

SK3T-4272 *z/OS Security Server RACF Collection*

This softcopy collection kit contains the Security Server library for z/OS for multiple releases in both BookManager and Portable Document Format (PDF) formats. It also contains z/OS software product documents that contain substantial RACF information. This collection does not contain licensed documents.

SK3T-7876 *IBM eServer™ zSeries Redbooks Collection*

This softcopy collection contains a set of documents called IBM® Redbooks® that pertain to zSeries® subject areas ranging from e-business application development and enablement to hardware, networking, Linux®, solutions, security, Parallel Sysplex® and many others.

SK2T-2177 *IBM Redbooks S/390 Collection*

This softcopy collection contains a set of documents called IBM Redbooks that pertain to S/390® subject areas ranging from application development and enablement to hardware, networking, security, Parallel Sysplex and many others.

RACF courses

The following RACF classroom courses are available in the United States:

H3917 *Basics of z/OS RACF Administration*

H3927 *Effective RACF Administration*

ES885 *Exploiting the Advanced Features of RACF*

ES840 *Implementing RACF Security for CICS*

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 documents known as IBM Redbooks® that can help you set up and use RACF. These documents 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 documents follows. Other documents 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.

GG24-4282	<i>Secured Single Signon in a Client/Server Environment</i>
GG24-4453	<i>Enhanced Auditing Using the RACF SMF Data Unload Utility</i>
GG26-2005	<i>RACF Support for Open Systems Technical Presentation Guide</i>
SG24-4704	<i>OS/390 Security Services and RACF-DCE Interoperation</i>
SG24-4820	<i>OS/390 Security Server Audit Tool and Report Application</i>
SG24-5158	<i>Ready for e-business: OS/390 Security Server Enhancements</i>
SG24-6840	<i>Communications Server for z/OS V1R2 TCP/IP Implementation Guide Volume 7: Security</i>

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 *ibm.servers.mvs.racf* newsgroup for discussion of RACF-related topics. You can find this newsgroup on news (NNTP) server *news.software.ibm.com* using your favorite news reader client.

Internet sources

The following resources are available through the Internet to provide additional information about the RACF library and other security-related topics:

- **Online library**

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

<http://www.ibm.com/systems/z/os/zos/bkserv/>

- **Redbooks**

The documents known as IBM Redbooks that are produced by the International Technical Support Organization (ITSO) are available at the following address:

<http://www.redbooks.ibm.com>

- **Enterprise systems security**

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

<http://www.ibm.com/systems/z/advantages/security/>

- **RACF home page**

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

<http://www.ibm.com/servers/eserver/zseries/zos/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, or go to www.ibm.com/servers/eserver/zseries/zos/racf/goodies.html.

The code is also available from [ftp.software.ibm.com](ftp://ftp.software.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 or tool you want to download:

```
cd eserver/zseries/zos/racf/
```

An announcement will be posted on the RACF-L discussion list and on newsgroup *ibm.servers.mvs.racf* whenever something is added.

Note: Some Web browsers and some FTP clients (especially those using a graphical interface) might have problems using [ftp.software.ibm.com](ftp://ftp.software.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.

The z/OS Basic Skills Information Center

The z/OS Basic Skills Information Center is a Web-based information resource intended to help users learn the basic concepts of z/OS, the operating system that runs most of the IBM mainframe computers in use today. The Information Center is

designed to introduce a new generation of Information Technology professionals to basic concepts and help them prepare for a career as a z/OS professional, such as a z/OS system programmer.

Specifically, the z/OS Basic Skills Information Center is intended to achieve the following objectives:

- Provide basic education and information about z/OS without charge
- Shorten the time it takes for people to become productive on the mainframe
- Make it easier for new people to learn z/OS.

To access the z/OS Basic Skills Information Center, open your Web browser to the following Web site, which is available to all users (no login required):
<http://publib.boulder.ibm.com/infocenter/zos/basics/index.jsp>

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 8:30 a.m. through 5:00 p.m. Eastern 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

Summary of changes

Summary of changes for SA22-7685-05 z/OS Version 1 Release 11

This document contains information previously presented in *z/OS Security Server RACF General User's Guide*, SA22-7685-04, which supports z/OS Version 1 Release 10.

New information

- Chapter 4, “How am I defined to RACF?” includes a new section “Finding out what distributed identity information RACF has about you” on page 27.

You may notice changes in the style and structure of some content in this document—for example, headings that use uppercase for the first letter of initial words only, and procedures that have a different look and format. The changes are ongoing improvements to the consistency and retrievability of information in our documents.

This document includes terminology, maintenance, and editorial changes. Technical changes or additions to the text are indicated by a vertical line to the left of the change.

Summary of changes for SA22-7685-04 z/OS Version 1 Release 10

This document contains information previously presented in *z/OS Security Server RACF General User's Guide*, SA22-7685-03, which supports z/OS Version 1 Release 9.

New information

- Chapter 4, “How am I defined to RACF?” includes a new section “Finding out what custom field information RACF has about you” on page 25.
- Chapter 4, “How am I defined to RACF?” describes the PHRASE ENVELOPED line in the LISTUSER output.
- In Chapter 4, “How am I defined to RACF?,” the section “Finding out what Kerberos information RACF has about you” on page 29 describes the KEY FROM field, which indicates whether the Network Authentication Service keys were derived from the user's password or password phrase.

This document includes terminology, maintenance, and editorial changes, including changes to improve consistency and retrievability.

Summary of changes for SA22-7685-03 z/OS Version 1 Release 9

This document contains information previously presented in *z/OS Security Server RACF General User's Guide*, SA22-7685-02, which supports z/OS Version 1 Release 8.

Changed information

- In Chapter 4, “How am I defined to RACF?,” the section “Finding out what Kerberos information RACF has about you” on page 29 shows additional encryption types stored in the KERB segment that LISTUSER might display.
- In Chapter 5, “Changing how you are defined to RACF,” the section “Changing your password phrase” on page 44 indicates that installations can choose to allow password phrases as short as 9 characters.

This document contains terminology, maintenance, and editorial changes, including changes to improve consistency and retrievability.

Chapter 1. What is RACF?

Resource Access Control Facility (RACF) is a security program. It is a component of the Security Server for z/OS. RACF controls what you can do on the z/OS operating system. You can use RACF to protect your resources. RACF protects information and other resources by controlling the access to those resources. RACF provides security by:

- Identifying and verifying users
- Authorizing users to access protected resources
- Recording and reporting access attempts

Identifying and verifying users

RACF identifies you when you log on to the operating system you want to use. It does so by requiring a user identification, the user ID—a unique identification string. RACF then verifies that you are the user you say you are by requesting and checking a password. Each RACF user ID has a unique password. You should be the only one who knows your password. That way, RACF can ensure personal accountability.

Note: Some applications support authentication via digital certificates or Kerberos. When accessing these applications you might not need to enter a user ID and password.

In addition to a password, you can also have an optional *password phrase*, which you can use instead of a password with applications that support password phrases. A password phrase is a string of characters that can be longer than a password, and can contain characters that are not allowed in a password, including blanks. It is intended to be secure, but easy to remember.

Note: Most applications do not support password phrases, and require that you use your password.

When you are first defined to RACF, your group or security administrator assigns you a user ID and a password. The password is usually temporary, but the security administrator can choose to assign you a non-temporary password. A temporary password enables you to log on to the system the first time. As soon as you log on, RACF requires you to supply a new password of your choice to replace the temporary password. Your password might expire after a certain time interval, so you might need to change it periodically. See “Changing your password” on page 43 for information on how to do this.

Note: Your password might need to satisfy certain installation-defined rules. For example, your password might need to be longer than five characters, and be made up of a mixture of alphabetic and numeric characters. Check with your system administrator or security administrator for the rules you should follow when you create a password.

You might also be assigned a password phrase. If so, the first time you log on using your password phrase RACF requires you to supply a new password phrase of your choice. Your password phrase might expire after a certain time interval, so you might need to change it periodically. For information on how to do this, see “Changing your password phrase” on page 44.

Authorizing users to access protected resources

RACF enables your organization to define individuals and groups who use the system RACF protects. For example, for a secretary in your organization, a security administrator uses RACF to define a user profile that defines the secretary's user ID, initial password, and other information.

A *group* is a collection of individuals who have common needs and requirements. For example, the secretaries for a whole department might be defined as one group.

RACF also enables an installation to define what authorities you have, or what authorities a group to which you belong has. RACF controls what you can do on the system. Some individuals have a great degree of authority, while others have little authority. The degree of authority you are given is based on what you need to do your job.

Besides defining user and group authorities, RACF protects resources. A *resource* is your organization's information stored in its computer system, such as a data set. For example, a secretary might have a data set as a resource. RACF provides a way to control who has authority to access a resource.

RACF stores information about users, groups, and resources in profiles. A *profile* is a record of RACF information that has been defined by the security administrator. There are user, group, and resource profiles.

Note: RACF protects some z/OS UNIX resources, such as files and directories. Security information about these resources is not stored in profiles, but in the z/OS UNIX file system, and it is administered using z/OS UNIX commands. For more information about z/OS UNIX resources, see *z/OS UNIX System Services User's Guide*.

Using information in its profiles, RACF authorizes access to certain resources. RACF applies user attributes, group authorities, and resource authorities to control use of the system.

- Your user profile provides your user attributes. User attributes describe what system-wide and group-wide access privileges you have to protected resources.
- Your group profile describes the kind of authority you as a group member have to access resources that belong to your group.
- The resources themselves have profiles describing the type of authority needed to use them.

The security administrator or someone in authority in your organization controls the information in your user profile, in group profiles, and in resource profiles. You, as the end user, control the information in profiles describing your own resources, such as your own data sets. You can protect your data by setting up resource profiles.

A *resource profile* can contain an access list as well as a default level of access authority for the resources it protects. An *access list* identifies the access authorities of specific users and groups, while the default level of access authority applies to anyone not specifically in the access list. You can specify the users you want on the access list and what authority they have to use your data. You can change your resource profiles, but you cannot change the user or group profiles, because they are established by the system administrator.

RACF enables you to perform security tasks. You can use RACF to see the authorities you have, to protect your resources with profiles you create, or to give other users the authority to access your resources. For example, you might want to let someone look at a data set that contains a program you are developing, but not be able to change that data set. In the data set's profile, you can add that person to the access list with the authority to view, but not change, your data. In this way, RACF helps you protect your work.

Recording and reporting access attempts

Besides uniquely identifying and authorizing you, RACF can record what you do on the system. It keeps track of what happens on the system so that your organization can monitor who is logged on the system at any time. RACF reports if persons have attempted to perform unauthorized actions. For example, RACF can record when someone who does not have the proper authority tries to use or change your data.

Chapter 2. Using RACF panels

If your installation has installed the RACF panels, you can use them to perform security tasks. To get to the RACF panels, enter the command:

ISPF

The Interactive System Productivity Facility (ISPF) primary menu appears. Choose option **R** for RACF.

Notes:

1. Although this is the usual way to access RACF panels, your installation might have implemented a different path. Check with your security administrator for more information.
2. From any panel, pressing PF1 leads you to a help screen.

When you choose option **R**, you see a screen that looks something like this:

```
                                RACF - SERVICES OPTION MENU

SELECT ONE OF THE FOLLOWING:

    1  DATA SET PROFILES
    2  GENERAL RESOURCE PROFILES
    3  GROUP PROFILES AND USER-TO-GROUP CONNECTIONS
    4  USER PROFILES AND YOUR OWN PASSWORD
    5  SYSTEM OPTIONS
    6  REMOTE SHARING FACILITY
    7  DIGITAL CERTIFICATES AND KEY RINGS

    99  EXIT

FOR SESSION MANAGER MODE, ENTER YES      ==> _____
      Licensed Materials - Property of IBM
      5647-A01 (C) Copyright IBM Corp. 1994, 1999
      All Rights Reserved - U.S. Government Users
      Restricted Rights, Use, Duplication or Disclosure
      restricted by GSA ADP Schedule Contract with IBM Corp.

OPTION ==>
F1=HELP      F2=SPLIT      F3=END      F4=RETURN      F5=RFIND      F6=RCHANGE
F7=UP        F8=DOWN        F9=SWAP     F10=LEFT      F11=RIGHT     F12=RETRIEVE
```

Figure 1. The RACF primary menu panel

The session manager mode prompt appears on this panel only if the session manager has been installed on your system.

You might need to know the panel ID for diagnosis purposes. To display the panel ID in the upper left part of the screen, enter the following ISPF command on the option line:

PANELID

You can access help information for the RACF panels. Help panels exist for each individual panel. If you have a question about the information you should provide on the panel, type **HELP** on the command line. The help panels give more information about the terms on the panel and the information you should enter.

Chapter 3. Using RACF commands

You can use RACF commands to perform security tasks. RACF commands enable you to find out how you are defined to RACF, how to protect your resources, how to change another user's access to your resources, and how to change the way RACF defines you. You can enter RACF commands directly in the foreground during a TSO command terminal session.

This book shows examples of RACF commands in uppercase letters. When you enter these commands from a terminal or workstation, you can use uppercase letters, lowercase letters, or both.

Note: You might not be able to do all of these tasks, depending on how your security administrator sets up RACF on your system.

RACF commands for general user tasks

Table 1 shows which command to use for each task and where it is described.

Table 1. RACF command table for general user tasks

Task	Command	Where described
Find out how you are defined to RACF	LISTUSER	16
Find out what CICS® information RACF has about you	LISTUSER <i>your-userid</i> CICS NORACF	24
Find out what custom field information RACF has about you	LISTUSER <i>your-userid</i> CSDATA NORACF	25
Find out what DCE information RACF has about you	LISTUSER <i>your-userid</i> DCE NORACF	28
Find out what distributed identity information RACF has about you	RACMAP	27
Find out what DFSMSdfp™ information RACF has about you	LISTUSER <i>your-userid</i> DFP NORACF	28
Find out what EIM information RACF has about you	LISTUSER <i>your-userid</i> EIM NORACF	28
Find out what Kerberos information RACF has about you	LISTUSER <i>your-userid</i> KERB NORACF	29
Find out what language information RACF has about you	LISTUSER <i>your-userid</i> LANGUAGE NORACF	30
Find out what information related to Lotus® Notes® RACF has about you	LISTUSER <i>your-userid</i> LNOTES NORACF	31
Find out what NetView® information RACF has about you	LISTUSER <i>your-userid</i> NETVIEW NORACF	31
Find out what OPERPARM information RACF has about you	LISTUSER <i>your-userid</i> OPERPARM NORACF	33
Find out what OpenExtensions information RACF has about you	LISTUSER <i>your-userid</i> OVM NORACF	33
Find out what TSO/E information RACF has about you	LISTUSER <i>your-userid</i> TSO NORACF	37
Find out what WORKATTR information RACF has about you	LISTUSER <i>your-userid</i> WORKATTR NORACF	38

Using RACF commands

Table 1. RACF command table for general user tasks (continued)

Task	Command	Where described
Find out what z/OS UNIX System Services (z/OS UNIX) information RACF has about you	LISTUSER <i>your-userid</i> OMVS NORACF	35
List all of your user ID associations	RACLINK LIST	39
List all of your user ID associations with a specific node, user ID, or both	RACLINK LIST(<i>node.userid</i>)	40
List all of your digital certificates	RACDCERT LIST	41
List all of your digital certificate key rings	RACDCERT LISTRING(*)	41
Change your password (<i>pw</i>)	PASSWORD PASSWORD(<i>current-pw new-pw</i>)	43
Change your password and password phrase interval	PASSWORD INTERVAL(<i>interval-you-want</i>)	43
	or PHRASE INTERVAL(<i>interval-you-want</i>)	
Change your password phrase (<i>pp</i>)	PASSWORD PHRASE (<i>current-pp new-pp</i>)	44
	or PHRASE PHRASE (<i>current-pp new-pp</i>)	
Log on to a group other than your default group	LOGON <i>userid</i> GROUP(<i>groupname</i>)	47
	Note: The LOGON command is a TSO command, not a RACF command.	
Log on with a security label other than your default security label	LOGON <i>userid</i> SECLABEL(<i>security-label</i>)	48
	Note: The LOGON command is a TSO command, not a RACF command.	
Allow another user to submit your jobs	PERMIT CLASS(SURROGAT) <i>userid</i> .SUBMIT ID(<i>surrogate-userid</i>) ACCESS(READ)	50
Enable your user IDs to have their passwords become synchronized as they are changed	RACLINK DEFINE(<i>target-node.target-userid</i>) PEER(PWSYNC)	52
	RACLINK APPROVE(<i>node.userid</i>)	
	Note: These commands need to be entered only once. All passwords are automatically changed after the password is changed for any one of the associated user IDs.	
Define a peer user ID association with password synchronization	RACLINK DEFINE(<i>target-node.target-userid</i>) PEER(PWSYNC)	52
Define a peer user ID association without password synchronization	RACLINK DEFINE(<i>target-node.target-userid</i>) PEER(NOPWSYNC)	52
Define a managed user ID association	RACLINK DEFINE(<i>target-node.target-userid</i>) MANAGED	53
Approve a user ID association	RACLINK APPROVE(<i>node.userid</i>)	53

Table 1. RACF command table for general user tasks (continued)

Task	Command	Where described
Delete a pending or existing user ID association	RACLINK UNDEFINE(<i>node.userid</i>)	54
Create a discrete profile to protect a cataloged data set	ADDSD ' <i>dataset-name</i> ' UACC(<i>access-authority</i>)	57
Create a discrete profile to protect an uncataloged data set	ADDSD ' <i>dataset-name</i> ' UNIT(<i>type</i>) VOLUME(<i>volume-serial</i>) UACC(<i>access-authority</i>)	57
Create a generic profile to protect a data set	ADDSD ' <i>dataset-name-with-generic-char.</i> ' UACC(<i>access-authority</i>) or ADDSD ' <i>dataset-name</i> ' UACC(<i>access-authority</i>) GENERIC	59
Find out how a data set is protected	LISTDSD DATASET(' <i>dataset-name</i> ') ALL or LISTDSD DATASET(' <i>dataset-name</i> ') ALL GENERIC	64
Check what data set profiles you have	SEARCH	69
Delete a data set profile	DELDSD ' <i>profile-name</i> '	69
Change a data set's universal access authority	ALTDSD ' <i>profile-name</i> ' UACC(<i>access-authority</i>)	73
Permit an individual or a group to use a data set	PERMIT ' <i>profile-name</i> ' ID(<i>userid groupname</i>) ACCESS(<i>level</i>)	74
Deny an individual or a group use of a data set	PERMIT ' <i>profile-name</i> ' ID(<i>userid groupname</i>) ACCESS(NONE) or PERMIT ' <i>profile-name</i> ' ID(<i>userid groupname</i>) DELETE	75
Search for general resource profile names	SEARCH CLASS(<i>classname</i>)	79
List the contents of general resource profiles	RLIST <i>classname profile-name</i>	80
Permit an individual or a group to use a general resource	PERMIT <i>profile-name</i> CLASS(<i>classname</i>) ID(<i>userid groupname</i>) ACCESS(<i>access-authority</i>)	81
Deny an individual or a group the use of a general resource	PERMIT <i>profile-name</i> CLASS(<i>classname</i>) ID(<i>userid groupname</i>) ACCESS(NONE) or PERMIT <i>profile-name</i> CLASS(<i>classname</i>) ID(<i>userid groupname</i>) DELETE	82

Getting online help for RACF commands

You can get online help for RACF commands; to do so, issue the following command:

```
HELP command-name
```

For example, to see online help for the PERMIT command, enter:

```
HELP PERMIT
```

To limit the information displayed, use the SYNTAX operand on the HELP command:

```
HELP command-name SYNTAX
```

For example, to see only the syntax of the PERMIT command, enter:

```
HELP PERMIT SYNTAX
```

For more information about the HELP command and other useful operands, see *z/OS Security Server RACF Command Language Reference*.

Escaping from a command prompt sequence

If you make a mistake while entering a RACF command during a TSO terminal session, you might receive IKJ messages such as INVALID KEYWORD and REENTER THIS OPERAND. These messages describe the syntax error and will prompt you to reenter the input. To end the prompting sequence, enter the requested information or press the attention interrupt key (PA1) to cancel the command.

Using command abbreviations

You can abbreviate an operand on a TSO command to the least number of characters that uniquely identify the operand. To avoid conflicts in abbreviations, it is a good practice to fully spell out all operands on commands that are hardcoded (for example, in programs and CLISTs).

Directing commands

The RACF remote sharing facility (RRSF) lets you direct most RACF commands to be processed on a node and user ID other than the one you are currently logged on to. You can also direct a command to the user ID you are currently logged on to. Directed commands run asynchronously; that is, the command issuer does not wait until the command completes processing, and results and output from the commands are returned to the command issuer in a data set. *z/OS Security Server RACF Command Language Reference* lists the commands that can be directed. See “User ID associations” on page 51 for information on creating the user ID associations necessary to direct commands. Also, you must have authorization to direct commands. If you are not sure whether you are authorized, contact your security administrator or see *z/OS Security Server RACF Security Administrator’s Guide* for more information.

You can use the AT keyword to direct allowed RACF commands to be processed under the authority of an associated user ID without actually logging on to that ID. Add the AT keyword to the end of any allowed RACF command and specify the node and user ID (*node.userid*) at which the command should be processed. A user

ID association is required for all commands directed to another node or user ID, but it is not required if you are directing the command to the user ID you are currently logged on to.

When you direct a command, the results are returned to you and are appended to the bottom of your RRSFLIST user data set. You receive a TSO SEND message telling you whether the directed command completed successfully or unsuccessfully. If you do not have an RRSFLIST user data set, RACF allocates one and adds the results. The RRSFLIST data set name is '*prefix.userid.RRSFLIST*', where *prefix* is your TSO prefix at the time you issued the command. If *prefix* matches *userid* or if you specified PROFILE NOPREFIX on the TSO PROFILE command, the data set name used is '*userid.RRSFLIST*'.

You are responsible for maintaining this data set. If your data set becomes full, the output is transmitted to your user ID. In order for RACF to append to your RRSFLIST user data set again, you must edit and delete some of the returned output in this data set. If your RRSFLIST user data set is in use when the RACF remote sharing facility tries to append the results, RACF waits for a brief time and tries again. This could cause the results of directed commands to be appended out of sequence with the output that was returned.

The following examples illustrate the format of the output produced by directed commands. The format of the output is the same for both your RRSFLIST data set and for the output transmitted when your data set is full. Figure 2 shows the format of output for this directed LISTGRP command:

```
LISTGRP (SYS1) AT(MVS03.SMITHJ)
```

Figure 3 shows the format of output for this directed ADDSD command:

```
ADDSD 'JWS.DEV*' AT(MVS02.JWS)
```

```
=====
LG issued at 09:14:32 on 02/02/98 was processed at MVS03.SMITHJ on
02/02/98 at 09:16:24

COMMAND ISSUED: LISTGRP (SYS1)

COMMAND OUTPUT:
INFORMATION FOR GROUP SYS1
SUPERIOR GROUP=NONE OWNER=SMITHJ
NO INSTALLATION DATA
NO MODEL DATA SET
TERMUACC

=====
```

Figure 2. A directed LISTGRP command: sample output

```
=====
ADDSD issued at 09:47:32 on 02/02/98 was processed at MVS02.JWS on
02/02/98 at 09:48:51

COMMAND ISSUED: ADDSD 'JWS.DEV*'

COMMAND OUTPUT:
IRRR008I Command succeeded. There are no messages.

=====
```

Figure 3. A directed ADDSD command: sample output

Automatic command direction

Automatic command direction, which is an extension of command direction, is useful primarily for keeping already-synchronized RACF profiles synchronized between two or more remote nodes. Every automatically directed command is processed on the node that originates the command; profiles in the RRSFDATA class identify the other nodes where the command should also be processed. Your RACF security administrator sets up these profiles. No user ID associations are required for automatic command direction. If user ID associations are defined, they are ignored during processing for automatic command direction.

An installation decides who should be notified of results and output from automatically directed commands, so you might or might not see output or TSO SEND messages from automatically-directed commands.

If you get output or notification that an automatically directed command failed, notify your RACF security administrator. This is an indication that the RACF profiles are no longer synchronized.

The format of the output for automatic command direction is similar to the output from directed commands, with one additional line for automatic command direction. Figure 4 shows the format of output for an automatically directed ADDUSER command. Figure 5 shows the format of output for an automatically directed RDEFINE command.

```
=====
ADDUSER issued at 10:42:33 on 04/03/98 was processed at NODEA.LAURIE
on 04/03/98 at 10:43:45
Command was propagated by automatic direction from NODEB.LAURIE

COMMAND ISSUED:  ADDUSER (ANDREW) PASSWORD() NAME('#####')
AUTHORITY(USE) NOSPECIAL UACC(NONE) NOOPERATIONS NOADSP NOGRPACC NOAUDITOR

COMMAND OUTPUT:
IRRR008I Command succeeded.  There are no messages.
=====
```

Figure 4. An automatically-directed ADDUSER command: sample output

```
=====
RDEFINE issued at 12:33:41 on 04/03/98 was processed at NODEA.LAURIE
on 04/03/98 at 12:35:02
Command was propagated by automatic direction from NODEB.LAURIE

COMMAND ISSUED:  RDEFINE AUTODIRECT.** UACC(NONE)

COMMAND OUTPUT:
ICH10102I AUTODIRECT.** ALREADY DEFINED TO CLASS RRSFDATA.
=====
```

Figure 5. An automatically-directed RDEFINE command: sample output

Getting help for RACF messages

If a RACF command fails, you receive a message. If you do not get a message ID, enter:

```
PROFILE MSGID
```

Then, reenter the RACF command that failed. The message appears with the message ID. Refer to *z/OS Security Server RACF Messages and Codes* for help if the message ID starts with ICH or IRR.

You can also use LookAt to find explanations of most messages. LookAt is an online message retrieval facility, and is not limited to RACF messages. For more information about LookAt, see the LookAt Web site at <http://www.ibm.com/servers/eserver/zseries/zos/bkserv/lookat/>.

Viewing notification messages

To see notification messages from command direction and password synchronization, enter:

```
PROFILE INTERCOM
```

To suppress notification messages from command direction and password synchronization, enter:

```
PROFILE NOINTERCOM
```

Notes:

1. RACF uses the INTERCOM setting at the time the directed command or password synchronization change occurred and if the setting was NOINTERCOM at that time, RACF does not issue a message after that command has processed.
2. If automatic command direction is active and your RACF security administrator has enabled notification for command issuers, the INTERCOM setting also controls notification messages from automatically directed commands.

Using RACF commands

Chapter 4. How am I defined to RACF?

To log on to a system, you must be defined to RACF. RACF records security information about you in a user profile. The profile contains information about when you last updated your password, what group you belong to, and what individual and group authority you have on the system. This chapter shows you how to find out how RACF has defined you to the system.

Finding out if you are defined to RACF

The RACF security administrator defines new RACF users and permits them to use the system and certain protected resources. When you are defined to RACF, your ability to use the system is defined at the same time. Being RACF-defined makes your identity known to RACF and describes your authority: what you can do and what resources you can use to do your job.

If you do not know your user ID, see your RACF security administrator or someone in authority at your installation, for example, a supervisor. Without a user ID you cannot use the system.

Note: If you are RACF-defined and this is the first time you have ever logged on to the system, you must change your password. After you have entered your assigned temporary password, you will receive a message saying that it has expired. Enter a new password of your choice, following the password rules set by your installation. See “Changing your password” on page 43 for information about changing your password periodically.

Log on to the system. Figure 6 shows a sample logon panel:

```
----- TSO/E LOGON -----  
  
Enter LOGON parameters below:                RACF LOGON parameters:  
Userid   ===> CLAIRE                          SECLABEL   ===>  
Password ===> _                               New Password ===>  
Procedure ===> PROC01                        Group Ident ===>  
Acct Nmbr ===> 123199  
Size     ===>  
Perform  ===>  
Command  ===>  
  
Enter an 'S' before each option desired below:  
-Nomail      -Nonotice      -Reconnect      -OIDcard  
  
PF1/PF13 ==> Help   PF3/PF15 ==> Logoff   PA1 ==> Attention   PA2 ==> Reshow  
You may request specific help information by entering a '?' in any entry field
```

Figure 6. A sample logon panel

Look at the right side of your logon panel. If the **New Password**, **Group Ident**, and optionally, the **SECLABEL** fields appear, you are defined to RACF.

Finding out how you are defined to RACF

As discussed in Chapter 1, “What is RACF?,” on page 1, RACF builds a description of you and your authority in a user profile. Each RACF-defined user has a user profile containing information about his or her identity, user attributes, group, and password. You belong to at least one group. This group is a default group to which your security administrator has assigned you. RACF has a profile defined for this group. This profile contains information about the group, its members, and the authority its members have to use the group’s resources.

To see a list of the information that RACF has about you and the group to which you belong, enter the command:

```
LISTUSER your-userid
```

or

```
LISTUSER
```

Note: If you issue the LISTUSER command and do not specify a user ID, information for your user ID is displayed.

Figure 7 on page 17 shows the fields that appear in the LISTUSER command output. “Understanding the information RACF has about you as a user” on page 17 and “Finding out what authority you have as a member of a group” on page 20 describe what this RACF information means. Figure 8 on page 23 and Figure 9 on page 24 show examples of LISTUSER command output.

```

USER=userid NAME=your-user-name OWNER=owner CREATED=yy.nnn
DEFAULT-GROUP=group PASSDATE=yy.nnn PASS-INTERVAL=nnn PHRASEDATE=yy.nnn
PASSWORD ENVELOPED=password envelope status
PHRASE ENVELOPED=password phrase envelope status
ATTRIBUTES=your operating privileges and restrictions
REVOKE DATE=date RESUME DATE=date
LAST-ACCESS=yy.nnn/hh:mm:ss

CLASS AUTHORIZATIONS=installation-defined classes where you can define
profiles

INSTALLATION-DATA=information your installation maintains about you
MODEL-NAME=profile used as a model for new data set profiles

LOGON ALLOWED (DAYS) (TIME)
-----
days you have access times you have access

GROUP=group AUTH=auth CONNECT-OWNER=owner CONNECT-DATE=yy.ddd

CONNECTS=nn UACC=uacc LAST-CONNECT=connect time

CONNECT ATTRIBUTES=your operating privileges as a group member

REVOKE DATE=date RESUME DATE=date

SECURITY-LEVEL=your installation-assigned security level

CATEGORY-AUTHORIZATION
your installation-assigned security categories

SECURITY-LABEL=your installation-assigned security label

```

Figure 7. LISTUSER output: description

Understanding the information RACF has about you as a user

As Figure 7 shows, RACF displays the following information when you issue the LISTUSER command.

USER

Your *userid* is the name by which the system knows you. It is frequently a combination of such identifying information as your name, initials, personnel number, or department.

NAME

Your name as recorded in your user profile.

OWNER

The user ID or group name of the owner of your user profile. The owner of your profile can modify your profile.

CREATED

The date you were defined to RACF.

Your RACF definition

DEFAULT-GROUP

RACF connects each user to at least one group. If you are a member of only one group, that group is your default group and that group name appears in this field.

If you belong to more than one group, and have no trouble accessing information belonging to the various groups to which you belong, you can ignore this field. If you have difficulty using group resources of a group to which you belong, log on again and specify the group to which you want to be connected at the logon panel. (If you do not specify the group, RACF assumes the group named in this field.)

PASSDATE

The date you last updated your password.

PASS-INTERVAL

The number of days your password, or password phrase if you have one, remains valid after you change it. If you try to use your password or password phrase after that interval, RACF considers it expired and you need to change it in order to logon successfully. The security administrator can set a system-level interval that overrides the interval shown for your user ID.

PHRASEDATE

The date you last updated your password phrase, or N/A if you do not have a password phrase.

PASSWORD ENVELOPED

Indicates whether or not your password is *enveloped*. An enveloped password is an encrypted copy of a password stored in the user profile that can be retrieved by authorized applications. The security administrator controls whether password enveloping is supported at an installation, and for which users.

PHRASE ENVELOPED

Indicates whether or not your password phrase is *enveloped*. An enveloped password phrase is an encrypted copy of a password phrase stored in the user profile that can be retrieved by authorized applications. The security administrator controls whether password phrase enveloping is supported at an installation, and for which users.

ATTRIBUTES

The system operating privileges and restrictions assigned to you. This field describes your system-wide attributes.

NONE Gives you no *special* operating privileges or restrictions; most users have this attribute. However, users with the NONE attribute can still use RACF. In fact, most other attributes allow extraordinary privileges, and generally only a few users or groups have these attributes.

SPECIAL

Gives you full authorization to modify all profiles in the RACF database and lets you perform all RACF functions except those requiring the AUDITOR attribute.

AUDITOR

Lets you audit the use of system resources, control the logging of detected accesses to resources, and create security reports.

OPERATIONS

Allows you to have full authorization to all RACF-protected data sets and to general resources that meet certain conditions (described in *z/OS Security Server RACF Security Administrator's Guide*).

OPERATIONS allows you to perform any maintenance operations, such as copying and reorganizing a RACF-protected resource.

GRPACC

Allows you to have the group data sets you allocate automatically accessible to other users in the specified group.

CLAUTH

Allows you to define profiles for any class specified in the class name.

ADSP Is the automatic data set protection attribute. If you have the ADSP attribute, RACF creates a discrete profile for every permanent DASD or tape data set you create. If your installation is using automatic direction of application updates and you have the ADSP attribute, you might be notified of the results and output from these application updates. See “Automatic direction of application updates” on page 90 for more information.

REVOKE

Prohibits a user from entering the system. (You should never see this attribute when you list your own profile.)

PASSPHRASE

Indicates that you have been assigned a password phrase in addition to a password. For more information about password phrases, see “Changing your password phrase” on page 44.

REVOKE DATE

This is the date on which RACF prevents you from using the system.

RESUME DATE

This is the date on which RACF allows you to use the system again.

LAST-ACCESS

This date is the last time you were on the system. RACF keeps records of all persons who have used the system, and what they have done, as well as recording unauthorized attempts to use the system.

CLASS AUTHORIZATIONS

Your installation assigns resources to various classes. The class appearing in this field is the class in which the user is authorized to assign RACF protection.

INSTALLATION-DATA

Additional information that your installation maintains about you and your authority. If you need help understanding anything in this field, see your RACF security administrator or the owner of your user profile. If NO-INSTALLATION-DATA appears in this field, your installation is not maintaining additional information.

MODEL-NAME

If a profile name appears in this field, the profile is used as a model when you create data set profiles that have your user ID as the high-level qualifier. If NO-MODEL-NAME appears in this field, no profile is being used as a model.

LOGON ALLOWED

The days of the week and hours in the day that RACF allows you to access the system from a terminal. These restrictions only limit the periods during which you can log on to the system. If you are working on the system and an end-time occurs, RACF does not force you off the system. Also, these logon restrictions do not apply to batch jobs; you can still submit a batch job at any time.

Your RACF definition

SECURITY-LEVEL

Your installation can define various security levels. The name appearing in this field is the security level assigned to you.

CATEGORY-AUTHORIZATION

Your installation can define various security categories. The names appearing in this field are the security categories assigned to you.

SECURITY-LABEL

Your installation can define various security labels. A security label is a name used to represent an association between a particular security level and certain security categories. The name appearing in this field is your default security label.

Note: When you specify the user ID on the LISTUSER command, the default security label from the user profile is displayed in the output. When you do not specify the user ID on the LISTUSER command, the security label you are currently logged on with is displayed in the output.

Finding out what authority you have as a member of a group

A group is a number of users defined together because of their common needs. For example, a group might be all the secretaries in a particular department. A group shares common access requirements to resources or has similar attributes within the system.

When you log on, RACF connects you to your default group. If you wish to log on to a group other than your default group, you can specify the group name when you log on. The group that you specify becomes your current connect group. When you are connected to a group, RACF allows you the privileges of the group.

You can receive this information about the groups to which you belong by using the following command.

```
LISTUSER your-userid
```

The information in the second part of the screen shown in Figure 7 on page 17 describes the RACF group or groups to which you belong and what you can do as a member of that group.

This section is repeated once for each RACF group of which you are a member. RACF uses the following terms to describe the group to which you belong and your authorities as a member of the group.

GROUP

The name of a group of which you are a member.

AUTH

The group authorities you have because you are a member of this group.

USE Allows you to enter the system under the control of the specified group. You can use any of the data sets the group can use.

CREATE

Allows you to RACF-protect group data sets and control who can access them. It includes the privileges of the USE authority.

CONNECT

Allows you to connect RACF-defined users to the specified group and assign these users the USE, CREATE, or CONNECT authority. It includes the privileges of the CREATE authority.

JOIN Allows you to define new users or groups to RACF and to assign group authorities. To define new users, you must also have the user attribute, CLAUTH(USER). JOIN authority includes all the privileges of the CONNECT authority.

CONNECT-OWNER

The owner of this group.

CONNECT-DATE

The date you were first connected to this group.

CONNECTS

The number of times you have been connected to this group.

UACC

The universal access authority for resources you create while connected to this group. If a user is not specifically listed in the access list describing a resource owned by the connect group, RACF looks at UACC and allows the user to use the resource in the manner specified in the UACC.

The UACC can be one of the following:

NONE Does not allow users to access the data set.

Attention

Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected data set can create a copy of it. As owner of the copied data set, that user has control of the security characteristics of the copied data set, and can downgrade it. For this reason, you might want to initially assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See "Permitting an individual or a group to use a data set" on page 74 for information on how to permit selected users or groups to access a data set.)

READ Allows users to access the data set for reading only. (Note that users who can read the data set can copy or print it.)

UPDATE

Allows users to read from, copy from, or write to the data set. UPDATE does not, however, authorize a user to delete, rename, move, or scratch the data set.

CONTROL

For VSAM data sets, CONTROL is equivalent to the VSAM CONTROL password; that is, it allows users to perform control-interval access (access to individual VSAM data blocks), and to retrieve, update, insert, or delete records in the specified data set.

For non-VSAM data sets, CONTROL is equivalent to UPDATE.

ALTER

ALTER allows users to read, update, delete, rename, move, or scratch the data set.

When specified in a discrete profile, ALTER allows users to read, alter, and delete the profile itself *including the access list*. However, ALTER does not allow users to change the owner of the profile.

Your RACF definition

When specified in a generic profile, ALTER gives users *no* authority over the profile itself, but allows users to create new data sets that are covered by that profile.

EXECUTE

For a private load library, EXECUTE allows users to load and execute, but not read or copy, programs (load modules) in the library.

Note: In order to specify EXECUTE for a private load library, you must ask for assistance from your RACF security administrator.

LAST-CONNECT

The last time you logged on or submitted a batch job with either the group as your default group or with the group explicitly specified. If you were never previously connected to the group, UNKNOWN is displayed.

CONNECT-ATTRIBUTES

The operating privileges and restrictions assigned to you when you are connected to this group. Connect attributes are also called group-level attributes. The connect (group-level) attributes are:

NONE Allows no *special* operating privileges or restrictions. Users with the NONE attribute can still use RACF. In fact, most other attributes allow extraordinary privileges, and generally only a few users or groups have these attributes.

SPECIAL

Gives you full authorization to all profiles in the RACF database and lets you perform all RACF functions except those requiring the AUDITOR attribute.

AUDITOR

Lets you audit the use of system resources, control the logging of detected accesses to resources, and create security reports.

OPERATIONS

Gives you full authorization to all RACF-protected data sets and to general resources that meet certain conditions (described in *z/OS Security Server RACF Security Administrator's Guide*). OPERATIONS lets you perform any maintenance operations, such as copying and reorganizing a RACF-protected resource.

GRPACC

Lets you have the group data sets that you allocate automatically accessible to other users in the specified group.

CLAUTH

Lets you define profiles for any class specified in the class name.

ADSP Is the automatic data set protection attribute. If you have the ADSP attribute, RACF creates a discrete profile for every permanent DASD or tape data set you create. If your installation is using automatic direction of application updates and you have the ADSP attribute, you might be notified of the results and output from these application updates. See "Automatic direction of application updates" on page 90 for more information.

REVOKE

Prohibits a user from entering the system. (You should never be able to see this attribute when you list your own profile.)

REVOKE DATE

This is the date on which RACF prevents you from using the system when you try to connect to the group.

RESUME DATE

This is the date on which RACF allows you to use the system again when you are connected to the group.

Examples of output of the LISTUSER command

The following examples show the output that is produced by the LISTUSER command for two typical RACF users.

Example 1:

G.L. Kline is an employee in the payroll department. G.L. Kline has a user ID of KLINE. If he entered the LISTUSER command, he would see output similar to that shown in Figure 8.

```

USER=KLINE   NAME=G.L.KLINE  OWNER=JONES   CREATED=96.091
DEFAULT-GROUP=PAYROLL  PASSDATE=06.124  PASS-INTERVAL= 30  PHRASEDATE=N/A
PASSWORD ENVELOPED=NO
PHRASE ENVELOPED=NO
ATTRIBUTES=NONE
REVOKE DATE=NONE  RESUME DATE=NONE
LAST-ACCESS=06.130/13:47:18
CLASS AUTHORIZATIONS=NONE
NO-INSTALLATION-DATA
NO-MODEL-NAME
LOGON ALLOWED      (DAYS)          (TIME)
-----
ANYDAY              ANYTIME
GROUP=PAYROLL  AUTH=USE  CONNECT-OWNER=JONES  CONNECT-DATE=96.091
CONNECTS= 05  UACC=NONE  LAST-CONNECT=06.130/13:47:18
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE  RESUME DATE=NONE
SECURITY-LEVEL=NONE SPECIFIED
CATEGORY-AUTHORIZATION
NONE SPECIFIED
SECURITY-LABEL=NONE SPECIFIED

```

Figure 8. LISTUSER output: example 1

In this example, user G.L. Kline is connected to only one group, PAYROLL. He has none of the possible user attributes, but can still use RACF. For example, Kline can create, change, and delete RACF profiles to protect his data sets.

Example 2:

D. Jones is an employee in the auditing department. D. Jones has a user ID of DJONES. If she enters the LISTUSER command, she sees output similar to that shown in Figure 9 on page 24.

Your RACF definition

```
USER=DJONES  NAME=D. JONES  OWNER=RYAN      CREATED=96.091
DEFAULT-GROUP=SEARCH  PASSDATE=06.124  PASS-INTERVAL= 30  PHRASEDATE=N/A
PASSWORD ENVELOPED=NO
PHRASE ENVELOPED=NO
ATTRIBUTES=AUDITOR
REVOKE DATE=NONE  RESUME DATE=NONE
LAST-ACCESS=06.114/13:47:18
CLASS AUTHORIZATIONS=NONE
NO-INSTALLATION-DATA
NO-MODEL-NAME
LOGON ALLOWED      (DAYS)          (TIME)
-----
ANYDAY              ANYTIME
GROUP=SEARCH AUTH=JOIN CONNECT-OWNER=WILL CONNECT-DATE=96.091
CONNECTS= 01  UACC=NONE  LAST-CONNECT=06.114/13:50:18
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE  RESUME DATE=NONE
GROUP=PAYROLL AUTH=CREATE CONNECT-OWNER=MILL CONNECT-DATE=96.091
CONNECTS= 00  UACC=READ  LAST-CONNECT=06.114/13:55:18
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE  RESUME DATE=NONE
SECURITY-LEVEL=NONE SPECIFIED
CATEGORY-AUTHORIZATION
NONE SPECIFIED
SECURITY-LABEL=NONE SPECIFIED
```

Figure 9. LISTUSER output: example 2

In this example, Jones is connected to two groups, SEARCH and PAYROLL. She has the AUDITOR system-wide attribute. Jones control access to her data sets and, as system AUDITOR, she can audit security controls and create security reports.

In the SEARCH group, Jones has JOIN group authority and can assign group authorities to members of the group. In the PAYROLL group, Jones has CREATE group authority and can create data set profiles to protect group data sets.

In the PAYROLL group, Jones also has assigned a UACC (universal access authority) of READ. If Jones logs on using PAYROLL as the current connect group, any data set profiles she creates have a UACC of READ (unless she specifies otherwise). For information on how to log on using a different connect group, see “Logging on to TSO/E with a group other than your default group” on page 47.

Finding out what CICS information RACF has about you

Your user profile might contain CICS information about you. RACF lists the following details from the CICS segment of the user profile:

- The classes assigned to this operator to which BMS messages are sent (OPCLASS)
- Whether or not the operator is forced off when an XRFSSOFF takeover occurs (XRFSSOFF)
- The operator identification (OPIDENT)
- The priority of the operator (OPPRTY)
- The time (in minutes or *hours:minutes*) that the operator is allowed to be idle before being signed off (TIMEOUT)
- Resource security level (RSL) keys, if any are assigned to the user (RSLKEYS). If 99 is displayed, this indicates that all RSL keys are assigned to the user (1–24, inclusive). If 0 is displayed, no RSL keys are assigned to the user.

- Transaction security level (TSL) keys, if any are assigned to the user (TSLKEYS). If 99 is displayed, this indicates that all TSL keys are assigned to the user (1–64, inclusive). If 0 is displayed, no TSL keys are assigned to the user.

Note: The RACF security administrator controls whether you can view all or some of the details of your CICS information.

The CICS information in the LISTUSER output has the following format:

```

USER=your user ID

CICS INFORMATION
-----
OPCLASS= operator classes
OPIDENT= operator class
OPPRTY= operator identification
TIMEOUT= idle time allowed
XRFSOFF= whether or not force-off will occur
RSLKEYS= RSL keys
TSLKEYS= TSL keys

```

Figure 10. LISTUSER output: description of the CICS information

Note: The ability to view and update CICS information can be controlled on a field by field basis; therefore, individual fields might not appear on your output.

To see the CICS information, issue the LISTUSER command as follows:

```
LISTUSER your-userid CICS NORACF
```

If there is CICS information in your profile, you see output similar to this:

```

USER=DJONES

CICS INFORMATION
-----
OPCLASS= 001
OPIDENT= ID2
OPPRTY= 00010
TIMEOUT= 12:34
XRFSOFF= NOFORCE
RSLKEYS= 00001 00003
TSLKEYS= 00001 00003

```

Figure 11. LISTUSER output: sample CICS information

Finding out what custom field information RACF has about you

Your user profile might contain installation-defined information about you. The security administrator can define custom fields unique to your installation, and specify for each field the type of data in the field, the length of the data, the output heading for the field in LISTUSER or LISTGRP output, the keyword name used for the field on TSO/E commands, and help text for the field. The custom field information is kept in the CSDATA segment of user and group profiles.

Note: The RACF security administrator controls whether you can view all or some of the details of your custom field information.

Your RACF definition

To see the custom field information contained in your user profile, issue the LISTUSER command as follows:

```
LISTUSER your-userid CSDATA NORACF
```

The output you see depends on the fields that the security administrator has defined and authorized you to view. For example, assume that the security administrator has defined the following custom fields for your installation:

- A flag field with the output heading “ACTIVE” that indicates whether or not an employee is active.
- A numeric field with the output heading “EMPLOYEE SERIAL” containing an employee's serial number.
- A character field with the output heading “HOME ADDRESS” containing an employee's home address.
- A character field with the output heading “HOME PHONE” containing an employee's home telephone number

You might see output similar to the following:

```
USER=DJONES  
  
CSDATA INFORMATION  
-----  
ACTIVE= YES  
EMPLOYEE SERIAL= 0000256400  
HOME ADDRESS= 14 Main Street, Anywhere, IL 01234  
HOME PHONE= 555-555-5555
```

Figure 12. LISTUSER output: sample custom field information

Finding out what DCE information RACF has about you

Your user profile might contain DCE information about you. RACF lists the following details from the DCE segment of the user profile:

- Your DCE principal name (DCENAME)
- Your DCE universal unique identifier (UUID)
- Your DCE home cell (HOMECCELL)
- The home cell's universal unique identifier (HOMEUUID)
- Whether you have single signon processing (AUTOLOGIN)

Note: The RACF security administrator controls whether you can view all or some of the details of your DCE information.

The DCE information in the LISTUSER output has the following format:

```
USER=your user ID  
  
DCE INFORMATION  
-----  
DCENAME= principal name  
UUID= universal unique identifier  
HOMECCELL= home cell  
HOMEUUID= home cell UUID  
AUTOLOGIN= YES|NO
```

Figure 13. LISTUSER output: description of the DCE information

To see the DCE information, issue the LISTUSER command as follows:

```
LISTUSER your-userid DCE NORACF
```

If your profile contains a DCE segment, you see output similar to this:

```
USER=MARTIN

DCE INFORMATION
-----
UUID= 004386ea-ebb6-1ec3-bcae-10005ac90feb
DCENAME= ELNINO
HOME CELL UUID= 003456aab-ecb7-7de3-ebda-95531ed63dae
HOMECELL= ../../hootie.scarol.ibm.com
AUTOLOGIN= YES
```

Figure 14. LISTUSER output: sample DCE information

Finding out what distributed identity information RACF has about you

Your user profile indicates whether any distributed identities have been associated with your RACF user ID. The associations, also referred to as *mappings*, are defined in profiles in the IDIDMAP class. Use the RACMAP command to see information about the distributed identities that are associated with your RACF user ID.

Note: The RACF security administrator controls whether you can use the RACMAP command to view the distributed identities associated with your user ID.

Enter any one of the following commands to see information about all of the distributed identities associated with your user ID. Because the ID keyword defaults to your RACF user ID, and the LISTMAP keyword is the default if you do not specify MAP or DELMAP, these commands all have the same effect:

- RACMAP
- RACMAP LISTMAP
- RACMAP ID(*your_RACF_user_ID*)
- RACMAP ID(*your_RACF_user_ID*) LISTMAP

If your RACF user ID was NET1ID, you would see output similar to the following:

```
Mapping information for user NET1ID:
Label: GeneralInternet ID Map
Distributed Identity User Name Filter:
>OU=Internet Demo,O=BobsMart Software Inc,L=Internet<
Registry name:
>ldaps//us.bobsmart.com<
```

Figure 15. Sample RACMAP output

- Label is a text string assigned to the mapping that is unique to the user ID.
- Distributed Identity User Name Filter is a filter for a distributed identity in X.500 distributed name format.
- Registry name is the name of the registry used to authenticate the distributed identity.

Finding out what DFSMSdfp information RACF has about you

Your user profile might contain DFSMSdfp information about you. The details RACF lists from the DFP segment of the user's profile are:

- The user's default data class (DATACLAS)
- The user's default management class (MGMTCLAS)
- The user's default storage class (STORCLAS)
- The identifier for a data set application (DATAAPPL)

Note: The RACF security administrator controls whether you can view all or some of the details of your DFSMSdfp information.

The DFSMSdfp information in LISTUSER output has the following format:

```
USER=DJONES

DFP INFORMATION
-----
MGMTCLAS= your default for management class
STORCLAS= your default for storage class
DATACLAS= your default for data class
DATAAPPL= your default for data application identifier
```

Figure 16. LISTUSER output: description of the DFSMSdfp information

Note: The ability to view and update DFSMSdfp information can be controlled on a field by field basis; therefore, any individual field might not appear on your output.

To see the DFSMSdfp information contained in your user profile, issue the LISTUSER command as follows:

```
LISTUSER your-userid DFP NORACF
```

If there is DFSMSdfp information in your profile, you see output similar to this:

```
USER=DJONES

DFP INFORMATION
-----
MGMTCLAS= DFPMG01
STORCLAS= DFPST01
DATACLAS= DFPDT01
DATAAPPL= DFPID01
```

Figure 17. LISTUSER output: sample DFSMSdfp information

Finding out what EIM information RACF has about you

Your user profile might contain Enterprise Identity Mapping (EIM) information about you. The details RACF lists from the EIM segment of the user's profile are:

- The name of a profile in the LDAPBIND class. The profile contains the name of an EIM domain and the bind information required to establish a connection with the EIM domain.

Note: The RACF security administrator controls whether you can view all or some of the details of your EIM information.

The EIM information in LISTUSER output has the following format:

```

USER=DJONES

EIM INFORMATION
-----
LDAPPROF= name of a profile in the LDAPBIND class

```

Figure 18. LISTUSER output: description of the EIM information

To see the EIM information contained in your user profile, issue the LISTUSER command as follows:

```
LISTUSER your-userid EIM NORACF
```

If there is EIM information in your profile, you see output similar to this:

```

USER=DJONES

EIM INFORMATION
-----
LDAPPROF= EIMDOMAINLOOKUP

```

Figure 19. LISTUSER output: sample EIM information

Finding out what Kerberos information RACF has about you

Your user profile might contain Kerberos information about you. The Network Authentication Service component of z/OS provides Kerberos support. The details RACF lists from the KERB segment of the user's profile are:

- The keys allowed for use (ENCRYPT).
- The local Kerberos principal name (KERBNAME).
- The maximum ticket life associated with this local principal (MAXTKTLFE).
- The current Network Authentication Service key version (KEY VERSION). If there is no Network Authentication Service key associated with your user ID, KEY VERSION is not displayed.
- The authenticator used to generate the current Network Authentication Service keys (KEY FROM).
 - PASSWORD indicates that the current keys were derived from your password.
 - PHRASE indicates that the current keys were derived from your password phrase.

Note: The RACF security administrator controls whether you can view all or some of the details of your Kerberos information.

The Kerberos information in LISTUSER output has the following format:

Your RACF definition

```
USER=DJONES

KERB INFORMATION
-----
KERBNAME= local Kerberos principle name
MAXTKLFE= maximum ticket life, in seconds
KEY FROM= PASSWORD | PHRASE
KEY VERSION= Network Authentication Service key version
KEY ENCRYPTION TYPE= [DES | NODES] [DES3 | NODES3] [DESD | NODESD]
                    [AES128 | NOAES128] [AES256 | NOAES256]
```

Figure 20. LISTUSER output: description of the Kerberos information

To see the Kerberos information contained in your user profile, issue the LISTUSER command as follows:

```
LISTUSER your-userid KERB NORACF
```

If there is Kerberos information in your profile, you see output similar to this:

```
USER=DJONES

KERB INFORMATION
-----
KERBNAME= KERB01
MAXTKLFE= 0000043200
KEY FROM= PASSWORD
KEY VERSION= 001
KEY ENCRYPTION TYPE= NODES DES3 NODESD AES128 NOAES256
```

Figure 21. LISTUSER output: sample Kerberos information

Finding out what language information RACF has about you

Your user profile might contain information about your language. RACF lists the following information from the LANGUAGE segment of the user profile:

- The user's primary language, if one has been specified (PRIMARY LANGUAGE)
- The user's secondary language, if one has been specified (SECONDARY LANGUAGE)

Note: The RACF security administrator controls whether you can view all or some of the details of your language information.

The language information in the LISTUSER output has the following format:

```
USER=your user ID

LANGUAGE INFORMATION
-----
PRIMARY LANGUAGE:  specified primary language
SECONDARY LANGUAGE: specified secondary language
```

Figure 22. LISTUSER output: description of the language information

Notes:

1. The ability to view and update language information can be controlled on a field by field basis; therefore, any individual field might not appear on your output.

2. The 3-character language code, and if defined, the 24-character language name is displayed. NOT SPECIFIED indicates that no language has been specified.

To see the language information, issue the LISTUSER command as follows:

```
LISTUSER your-userid LANGUAGE NORACF
```

If there is language information in your user profile, you see output similar to this:

```
USER=DJONES  
  
LANGUAGE INFORMATION  
-----  
PRIMARY LANGUAGE: ENU  
SECONDARY LANGUAGE: DEU
```

Figure 23. LISTUSER output: sample language information

Finding out what Lotus Notes information RACF has about you

Your user profile might contain information about you related to Lotus Notes. RACF lists the following information from the LNOTES segment of the user profile:

- Your Lotus Notes short name (SNAME)

Note: The RACF security administrator controls whether you can view your information related to Lotus Notes.

The information related to Lotus Notes in the LISTUSER output has the following format:

```
USER=your user ID  
  
LNOTES INFORMATION  
-----  
SNAME= Lotus Notes short name
```

Figure 24. LISTUSER output: description of the information related to Lotus Notes

To see the Lotus Notes information, issue the LISTUSER command as follows:

```
LISTUSER your-userid LNOTES NORACF
```

If your profile contains an LNOTES segment, you see output similar to this:

```
USER=MARTIN  
  
LNOTES INFORMATION  
-----  
SNAME= JMARTIN
```

Figure 25. LISTUSER output: sample Lotus Notes information

Finding out what NetView information RACF has about you

Your user profile might contain NetView information about you. The details RACF lists from the NetView segment of the user profile are:

- Command or command list to be processed at logon (IC)
- MCS extended console name (CONSNAME)

Your RACF definition

- Type of security check (CTL)
- Whether unsolicited messages will be received (MSGRECVR)
- Scope classes (OPCLASS)
- NetView programs in another NetView domain for which operator has authority (DOMAINS)
- Whether administrator authority is present for the NetView Graphic Monitor Facility (NGMFADMN)
- NetView Graphic Monitor Facility view span options (NGMFVSPN)

Note: The RACF security administrator controls whether you can view all or some of the details of your NetView information.

The NetView information in the LISTUSER output has the following format:

```
USER=your user ID

NETVIEW INFORMATION
-----
IC= command or command list information
CONSNAME= MCS extended console name
CTL= type of security check
MSGRECVR= whether unsolicited messages will be received
OPCLASS= scope classes
DOMAINS= domains
NGMFADMN= whether administrator authority is present
NGMFVSPN= authority to display NetView management console views
            and resources within views
```

Figure 26. LISTUSER output: description of the NetView information

Note: The ability to view and update NetView information can be controlled on a field by field basis; therefore, any individual field might not appear on your output.

To see the NetView information, issue the LISTUSER command as follows:

```
LISTUSER your-userid NETVIEW NORACF
```

If there is NetView information in your user profile, you see output similar to this:

```
USER=DJONES

NETVIEW INFORMATION
-----
IC= START
CONSNAME= DJONES1
CTL= GLOBAL
MSGRECVR= YES
OPCLASS= 1,2
DOMAINS= D1,D2
NGMFADMN= YES
NGMFVSPN= VNNN
```

Figure 27. LISTUSER output: sample NetView information

Finding out what OpenExtensions information RACF has about you

Your user profile might contain OpenExtensions information about you. (OpenExtensions runs on z/VM®.) The details RACF lists from the OVM segment of the user profile are:

- The user identifier (UID)
- The initial directory path name (HOME)
- The program path name (PROGRAM)
- The file system root directory (FSROOT)

Note: The RACF security administrator controls whether you can view all or some of the details of your OVM segment information.

The OpenExtensions information in the LISTUSER output has the following format:

```
USER=your user ID

OVM INFORMATION
-----
UID= user identifier
HOME= initial directory path name
PROGRAM= program path name
FSROOT= file system root directory
```

Figure 28. LISTUSER output: description of the OpenExtensions information

To see the OVM information, issue the LISTUSER command as follows:

```
LISTUSER your-userid OVM NORACF
```

If your profile contains an OVM segment, you see output similar to this:

```
USER=MARTIN

OVM INFORMATION
-----
UID= 0000000035
HOME= /u/martin
PROGRAM= /u/martin/bin/myshell
FSROOT= ../VMBFS:SERVER7:MARTIN/
```

Figure 29. LISTUSER output: OpenExtensions information (example 1)

If the OVM segment does not exist, you see output similar to this:

```
USER=MARTIN

NO OVM INFORMATION
```

Figure 30. LISTUSER output: OpenExtensions information (example 2)

Finding out what OPERPARM information RACF has about you

Your user profile might contain initial information used when you enter an extended MCS console session. The details RACF lists from the OPERPARM segment of the user profile are:

- Console recovery group (ALTGRP). This field is no longer used; consoles ignore it.

Your RACF definition

- Operator authority (AUTH)
- System name for commands from this console (CMDSYS)
- Whether and what kind of delete operator messages are received (DOM)
- Searching key (KEY)
- Message level information (LEVEL)
- Whether system command responses are logged (LOGCMDRESP)
- Message format (MFORM)
- Whether this console is assigned a migration ID (MIGID). This field is no longer used; consoles ignore it.
- Event information (MONITOR)
- The system from which this console can receive undirected messages from (MSCOPE)
- Routing code information (ROUTCODE)
- Storage information (STORAGE)
- Whether this console can receive undeliverable messages (UD). This field is no longer used; consoles ignore it.
- Whether the extended console can receive messages that have been automated by the NetView Message Processing Facility (MPF) in the sysplex (AUTO)
- Whether this console is to receive messages that are directed to hard copy (HC)
- Whether this console should receive messages that are directed to console ID zero (the internal console) (INTIDS)
- Whether this console is to receive messages that are directed to “unknown” console IDs. These are typically one-byte console IDs that the system cannot unambiguously resolve. (UNKNIDS)

Note: The RACF security administrator controls whether you can view all or some of the details of your OPERPARM information.

The OPERPARM information in the LISTUSER output has the following format:

```
USER=your user ID

OPERPARM INFORMATION
-----
STORAGE= storage information
AUTH= operator authority
AUTO= automated messages
ROUTCODE= routing code information
LEVEL= message level information
MFORM= message format
MONITOR= event information
LOGCMDRESP= whether system command responses are logged
MIGID= if a migration ID is assigned
DOM= whether and what kind of delete operator messages are received
KEY= searching key
CMDSYS= system name for this console's commands
MSCOPE= the system this console can receive undirected messages from
UD= whether this console can receive undeliverable messages
ALTGRP= console recovery group
HC= YES | NO
INTIDS= YES | NO
UNKNIDS= YES | NO
```

Figure 31. LISTUSER output: description of the OPERPARM information

Notes:

1. The ability to view and update OPERPARM information can be controlled on a field by field basis; therefore, any individual field might not appear on your output.

- If there is no information in a field in the user profile for this segment then the field name is not displayed. However, if no value was specified for STORAGE when the OPERPARM segment was added to the user profile, "STORAGE=0" appears in the listing.

To see the OPERPARM information, issue the LISTUSER command as follows:

```
LISTUSER your-userid OPERPARM NORACF
```

If there is OPERPARM information in your user profile, you see output similar to this:

```
USER=DJONES

OPERPARM INFORMATION
-----
STORAGE= 00002
AUTH= IO
AUTO= YES
ROUTCODE= ALL
LEVEL= ALL
MFORM= T J M
MONITOR= JOBNAMEST SESST
LOGCMDRESP= NO
MIGID= YES
DOM= NORMAL
KEY= MSC2
CMDSYS= SYS1
MSCOPE= *ALL
UD= YES
ALTGRP= BACKUP
HC= NO
INTIDS= NO
UNKNIDS= NO
```

Figure 32. LISTUSER output: sample OPERPARM information

Finding out what z/OS UNIX information RACF has about you

Your user profile might contain z/OS UNIX System Services information about you. The details RACF lists from the OMVS segment of the user profile are:

- The z/OS UNIX user identifier (UID)
- The initial directory path name (HOME)
- The program path name (PROGRAM)
- The CPU time, in seconds, that the user's processes can use (CPUTIMEMAX)
- The address space region size, in bytes, that the user's processes can use (ASSIZEMAX)
- The maximum number of active or open files that the user can have (FILEPROCMAx)
- The maximum number of active processes that the user can have (PROCUSERMAX)
- The maximum number of threads that the user can have (THREADSMAX)
- The maximum amount of space, in pages, that the user can map in storage (MMAPAREAMAX)
- The maximum number of bytes of nonshared memory that can be allocated by the user (MEMLIMIT)
- The maximum number of bytes of shared memory that can be allocated by the user (SHMEMMAX)

Your RACF definition

Note: The RACF security administrator controls whether you can view all or some of the details of your z/OS UNIX information.

The z/OS UNIX information in the LISTUSER output has the following format:

```
USER=your user ID

OMVS INFORMATION
-----
UID= your z/OS UNIX user identifier
HOME= initial directory path name
PROGRAM= program path name
CPUTIMEMAX= CPU time, in seconds, your processes can use
ASSIZEMAX= address space region size, in bytes, your processes can use
FILEPROCMAX= maximum number of active or open files you can have
PROCUSERMAX= maximum number of active processes you can have
THREADSMAX= maximum number of threads you can have
MMAPAREAMAX= maximum number of pages you can map in storage
MEMLIMIT= a numeric value followed by one of the following multipliers:
           M = megabyte (1 048 576)
           G = gigabyte (1 073 741 824)
           T = terabyte (1 099 511 627 776)
           P = petabyte (112 589 990 842 624)
SHMEMMAX= a numeric value followed by one of the following multipliers:
           M = megabyte (1 048 576)
           G = gigabyte (1 073 741 824)
           T = terabyte (1 099 511 627 776)
           P = petabyte (112 589 990 842 624)
```

Figure 33. LISTUSER output: description of the z/OS UNIX information

Notes:

1. If there is no information in the HOME or PROGRAM field in the user's profile for this segment, the field name is not displayed.
2. If UID was not specified when the OMVS segment was added to the user profile, the word NONE appears in the listing.
3. If there is no information in the CPUTIMEMAX, ASSIZEMAX, FILEPROCMAX, PROCUSERMAX, THREADSMAX, or MMAPAREAMAX field for this segment in the user's profile, the word NONE appears in the listing, and your system uses its system-level value for the field.
4. The ability to view and update z/OS UNIX information can be controlled on a field-by-field basis; therefore, any individual field might not appear on your output.

To see the z/OS UNIX information, issue the LISTUSER command as follows:

```
LISTUSER your-userid OMVS NORACF
```

If your profile contains an OMVS segment, you see output similar to this:

```

USER=CSMITH

OMVS INFORMATION
-----
UID= 0000000024
HOME= /u/CSMITH
PROGRAM= /u/CSMITH/bin/myshell
CPUTIMEMAX= 0010000000
ASSIZEMAX= NONE
FILEPROCMAX= 0000050000
PROCUSERMAX= NONE
THREADSMAX= NONE
MMAPAREAMAX= 0016777216
MEMLIMIT= 1G
SHMEMMAX= 5M

```

Figure 34. LISTUSER output: z/OS UNIX information (example 1)

If only the UID field has a value in the OMVS segment of your profile, you see output similar to this:

```

USER=CSMITH

OMVS INFORMATION
-----
UID= 0000000024
CPUTIMEMAX= NONE
ASSIZEMAX= NONE
FILEPROCMAX= NONE
PROCUSERMAX= NONE
THREADSMAX= NONE
MMAPAREAMAX= NONE

```

Figure 35. LISTUSER output: z/OS UNIX information (example 2)

Finding out what TSO/E information RACF has about you

Your user profile might contain TSO/E information about you. The details RACF lists from the TSO segment of the user profile are:

- The user's default job class (JOBCLASS)
- The user's default message class (MSGCLASS)
- The user's default hold class (HOLDCLASS)
- The user's default system output class (SYSOUTCLASS)
- The user's default account number (ACCTNUM)
- The user's logon procedure name (PROC)
- The user's default region size (SIZE)
- The user's maximum region size (MAXSIZE)
- The unit name (UNIT)
- The destination ID for SYSOUT data sets (DEST)
- Optional user data (USERDATA)
- The user's security label (SECLABEL)
- The TSO command to be processed at logon time (COMMAND)

Note: The RACF security administrator controls whether you can view all or some of the details of your TSO information.

The TSO/E information in LISTUSER output has the following format:

Your RACF definition

```
USER=your user ID

TSO INFORMATION
-----
ACCTNUM= default account number
DEST= default SYSOUT destination
HOLDCLASS= default hold class
JOBCLASS= default job class
MSGCLASS= default message class
PROC= default LOGON procedure
SIZE= default region size
MAXSIZE= default maximum region size
SYSOUTCLASS= default SYSOUT class
UNIT= default unit
USERDATA= user data
SECLABEL= TSO security label
COMMAND= TSO command processed at logon time
```

Figure 36. LISTUSER output: description of the TSO/E information

Notes:

1. The ability to view and update TSO information can be controlled on a field by field basis; therefore, any individual field might not appear on your output.
2. If there is no information in the fields of the TSO segment, the field name is not displayed (with the exception of SIZE, MAXSIZE, and USERDATA).

To see the TSO/E information contained in your user profile, issue the LISTUSER command as follows:

```
LISTUSER your-userid TSO NORACF
```

If there is TSO/E information in your profile, you see output similar to this:

```
USER=DJONES

TSO INFORMATION
-----
ACCTNUM= D5888P
DEST= LOCAL
HOLDCLASS= H
JOBCLASS= C
MSGCLASS= R
PROC= PROC01
SIZE= 0001024
MAXSIZE= 0004096
SYSOUTCLASS= J
UNIT= SYSDA
USERDATA= 1F09
SECLABEL= SYSLOW
```

Figure 37. LISTUSER output: sample TSO/E information

Finding out what WORKATTR information RACF has about you

Your user profile might contain work attribute information about you. The details RACF lists from the WORKATTR segment of the user profile are:

- The user name on SYSOUT (WANAME)
- The building on SYSOUT (WABLDG)
- The department on SYSOUT (WADEPT)
- The room on SYSOUT (WAROOM)
- Address lines 1, 2, 3 and 4 on SYSOUT (WAADDR1, WAADDR2, WAADDR3, WAADDR4)

- The account number (WAACCNT)

Note: The RACF security administrator controls whether you can view all or some of the details of your work attribute information.

The WORKATTR information in the LISTUSER output has the following format:

```

USER=your user ID

WORKATTR INFORMATION
-----
WANAME= user name
WABLDG= building
WADEPT= department
WAROOM= room
WAADDR1= address line 1
WAADDR2= address line 2
WAADDR3= address line 3
WAADDR4= address line 4
WAACCNT= account number

```

Figure 38. LISTUSER output: description of the WORKATTR information

To see the WORKATTR information, issue the LISTUSER command as follows:

```
LISTUSER your-userid WORKATTR NORACF
```

If your profile contains a WORKATTR segment, you see output similar to this:

```

USER=MARTIN

WORKATTR INFORMATION
-----
WANAME= Martin W. Gilfeather
WABLDG= 025
WADEPT= 58HA
WAROOM= 6W11
WAADDR1= Boices Dairy Farms
WAADDR2= 1 Neighborhood Road
WAADDR3= Kingston, New York
WAADDR4= 12401
WAACCNT= 040362

```

Figure 39. LISTUSER output: sample WORKATTR information

Finding out if your password is synchronized with other IDs

Your user profile might indicate if your password is being synchronized with other user IDs through user ID associations; see “Finding out what user ID associations are defined for you” for more information. Or, automatic password direction might be synchronizing your password changes without user ID associations; for more information, see “Automatic password direction” on page 46.

Finding out what user ID associations are defined for you

Your user profile might contain information about user ID associations defined for your user ID. The details RACF lists from the user profile are:

- Type of user ID association
- Node and user ID that are associated with you
- Whether password synchronization is in effect

Your RACF definition

- Status of the association

Note: User IDs do not need the same password to request an association. Passwords are synchronized automatically when either of the associated user IDs changes a password after the peer association with password synchronization has been established.

To see the information about your user ID associations, issue the RACLINK command as follows:

```
RACLINK LIST
```

If there are associations defined for your user ID, you see output similar to this:

```
ASSOCIATION information for user ID JUAN on node MVS01
at 09:27:12 on 07/16/98:
```

Association Type	Node.userid	Password Sync	Association Status
PEER OF	MVS03.JDOE	YES	ESTABLISHED
PEER OF	MVS04.JUAN	YES	ESTABLISHED
PEER OF	MVS01.SMITH	NO	PENDING APPROVAL BY SMITH
MANAGED BY	MVS04.SECADM	N/A	ESTABLISHED
MANAGER OF	MVS03.OPER2	N/A	ESTABLISHED
MANAGER OF	MVS03.MIKE	N/A	PENDING APPROVAL BY MIKE

Figure 40. RACLINK LIST output: user ID association information (example 1)

To see all your user ID associations defined with user IDs on node MVS03, enter the following command:

```
RACLINK LIST(MVS03.*)
```

The requesting user ID JUAN receives the following output:

```
ASSOCIATION information for user ID JUAN on node MVS01
at 10:02:54 on 07/16/98:
```

Association Type	Node.userid	Password Sync	Association Status
PEER OF	MVS03.JDOE	YES	ESTABLISHED
MANAGER OF	MVS03.OPER2	N/A	ESTABLISHED
MANAGER OF	MVS03.MIKE	N/A	PENDING APPROVAL BY MIKE

Figure 41. RACLINK LIST output: user ID association information (example 2)

To see all the user ID associations defined with your user ID JUAN on all nodes, enter the following command:

```
RACLINK LIST(*.JUAN)
```

The requesting user ID, JUAN, receives the following output:

```
ASSOCIATION information for user ID JUAN on node MVS01
at 10:22:34 on 07/16/98:
```

Association Type	Node.userid	Password Sync	Association Status
-----	-----	-----	-----
PEER OF	MVS04.JUAN	YES	ESTABLISHED

Figure 42. RACLINK LIST output: user ID association information (example 3)

Automatic registration of digital certificates

You might be able to use automatic registration of digital certificates, if this function has been enabled and you have been authorized to use it. To find out, check with your RACF security administrator or your Web administrator.

With automatic registration of digital certificates, your RACF user ID can be associated with a digital certificate through the WebSphere® Application Server. Your installation might provide a registration page on the Web. This Web page prompts for the registration of the certificate for your RACF user ID. When you click on the registration box on this Web page, a secure session is set up using the Secure Sockets Layer (SSL) and your digital certificate. You are then prompted for your RACF user ID and password. At this point, the registration process is ready to begin.

Listing your digital certificate information

You might be able to list the digital certificates and key rings associated with your user ID, as shown in the following examples.

User NETBOY requests the listing of his Savings Account digital certificate to ensure it has been defined, and that it is marked trusted. He has READ authority to the FACILITY class profile IRR.DIGTCERT.LIST. He issues the RACDCERT command with the LIST operand, specifying the label to identify his certificate:

```
RACDCERT LIST(LABEL('Savings Account'))
```

and receives the following output:

```
Digital certificate information for user NETBOY:
```

Label: Savings Account
Status: TRUST
Serial Number:
>5D666C20207A6638727A413872D8413B<
Issuer's Name:
>OU=BobsBank Savers.O=BobsBank.L=Internet<
Subject's Name:
>CN=S.S.Smith.OU=Digital ID Class 1 - NetScape.OU=BobsBank Class 1 - S<
>avingsAcct.O=BobsBank.L=Internet<

Figure 43. Example: listing your digital certificate information

User GEORGEM requests a listing of his key rings. He has three key rings with certificates and one key ring that has no certificates. He has READ authority to the

Your RACF definition

FACILITY class profile IRR.DIGTCERT.LIST. He issues the RACDCERT command with the LISTRING operand, specifying * to list all of his key rings:

```
RACDCERT LISTRING(*)
```

and receives the following output:

```
Digital ring information for user GEORGEM:

Ring:
>GEORGEMsNewRing01<
Certificate Label Name          Cert Owner    USAGE        DEFAULT
-----
New Cert Type - Ser # 00       ID(GEORGEM)  PERSONAL     YES
New Type Cert - VsignC1       ID(GEORGEM)  CERTAUTH     NO
New Type Cert - VsignC2       ID(GEORGEM)  SITE         NO
65                             ID(JOHNP)    PERSONAL     NO

Ring:
>GEORGEMsRing<
Certificate Label Name          Cert Owner    USAGE        DEFAULT
-----
GEORGEM's Cert # 48           ID(GEORGEM)  PERSONAL     NO
GEORGEM's Cert # 84           ID(GEORGEM)  PERSONAL     NO
New Cert Type - Ser # 00       ID(GEORGEM)  PERSONAL     YES

Ring:
>GEORGEMsRing#2<
Certificate Label Name          Cert Owner    USAGE        DEFAULT
-----
GEORGEM's Cert # 84           ID(GEORGEM)  PERSONAL     NO
GEORGEM's Cert # 48           ID(GEORGEM)  PERSONAL     NO

Ring:
>GEORGEMsRing#3<
*** No certificates connected ***
```

Figure 44. Listing your digital key ring information

If you are unable to issue the RACDCERT command, check with your RACF security administrator to get authorization.

Chapter 5. Changing how you are defined to RACF

You can change some of the ways you have been defined on the system by doing any or all of the tasks described in this chapter.

Changing your password

Your user ID identifies you to RACF and your password verifies your identity. You have to change your password after a certain interval of time to help ensure that it is known only to you. You can change the time interval between required password changes at the time you change your password.

Note: You can also change your password while logging on to the system. This is the most common way of changing your password. See “Finding out if you are defined to RACF” on page 15.

If you have multiple user IDs, you can keep your passwords automatically synchronized on the same system or across multiple systems by defining peer user ID associations with password synchronization enabled between your user IDs. See “Synchronizing your passwords and password phrases” on page 45 for additional information. An installation can also maintain the synchronization of user passwords between the same user IDs on different nodes by using automatic password direction. See “Automatic password direction” on page 46 for additional information.

RACF has the following rules for passwords:

- The length can be 1 to 8 characters.
- Valid characters are alphabetic uppercase (A–Z), numeric (0–9), and national (# (X'7B'), @ (X'7C'), and \$ (X'5B')). If your installation supports mixed case passwords, alphabetic lowercase characters (a-z) are also accepted in passwords. If your installation does not support mixed case passwords, any lowercase characters that you enter for your password are folded to uppercase. If you don't know whether mixed case passwords are supported, ask your security administrator.

In addition, your installation has password rules. If you do not know the rules, choose a password following the format of your current password. RACF might not allow you to reuse a previous password. Ask your RACF security administrator for an explanation of your installation's rules for passwords.

To change your password, enter the PASSWORD command with the PASSWORD keyword as follows:

```
PASSWORD PASSWORD(current-password new-password)
```

For example, if your installation supports mixed case passwords, to change your password from “subject” to “testers”, type:

```
PASSWORD PASSWORD(subject testers)
```

If your installation does not support mixed case passwords, RACF folds passwords that you enter to uppercase. In that case, the command shown changes your password from “SUBJECT” to “TESTERS”.

To change your password interval (that is, the time allowed before you are required to change your password again), enter the PASSWORD command with the INTERVAL keyword as follows:

Changing your system definitions

```
PASSWORD INTERVAL(interval-you-want)
```

For example, to change your password interval to 15 days, enter the following command:

```
PASSWORD INTERVAL(15)
```

At the end of 15 days, RACF requires you to change your current password.

RACF allows the interval to be in the range of 1 to 254 days. Your installation chooses its own interval in this range. You can change your password interval to a shorter length of time than your installation requires but you cannot specify a longer interval. For example, if your installation has a password interval of 30 days, you can change the interval to any number from 1 to 30 but you cannot change your password interval to 45 days.

If you do not know your current password interval, enter the LISTUSER command and check the PASS-INTERVAL field. For more information, see “Understanding the information RACF has about you as a user” on page 17.

To change your password and password interval, enter the PASSWORD command with the PASSWORD and INTERVAL keywords as follows:

```
PASSWORD PASSWORD(current-password new-password) INTERVAL(interval)
```

For example, to change the password from “subject” to “testers”, and the interval to 15 days, enter the following command:

```
PASSWORD PASSWORD(subject testers) INTERVAL(15)
```

Changing your password phrase

Your password phrase is an alternative to your password for verifying your identity. You have to change your password phrase after a certain interval of time to help ensure that it is known only to you. The interval is the same one that determines when you must change your password. You can change the time interval between required password and password phrase changes at the time you change your password phrase.

If you have multiple user IDs, you can keep your password phrases automatically synchronized on the same system or across multiple systems by defining peer user ID associations with password synchronization enabled between your user IDs. See “Synchronizing your passwords and password phrases” on page 45 for additional information. An installation can also maintain the synchronization of user password phrases between the same user IDs on different nodes by using automatic password direction. See “Automatic password direction” on page 46 for additional information.

RACF has the following rules for password phrases:

- The length can be 14 to 100 characters.

Note: Your installation can choose to allow password phrases as short as 9 characters. Check with your security administrator or system programmer to find out if the lower limit has been implemented.

- The user ID (as sequential upper case characters or sequential lower case characters) can not be part of the password phrase
- At least 2 alphabetic characters must be specified (A - Z, a - z)

- At least 2 non-alphabetic characters must be specified (numerics, punctuation, special characters)
- Valid characters are:
 - Alphabetic uppercase (A–Z) and lowercase (a–z)
 - Numeric (0–9)
 - National (# (X'7B'), @ (X'7C'), and \$ (X'5B'))
 - Punctuation
 - Special
 - Blank
- No more than 2 consecutive characters can be identical.

RACF might not allow you to reuse a previous password phrase.

Your installation might have additional rules for password phrases. Ask your RACF security administrator whether your installation has additional rules.

To change your password phrase, enter the PASSWORD or PHRASE command with the PHRASE keyword as follows:

```
PASSWORD PHRASE ('current-password-phrase' 'new-password-phrase')
```

or

```
PHRASE PHRASE ('current-password-phrase' 'new-password-phrase')
```

The current and new password phrases must have different values. Note that the password phrases must be entered in quotes. TSO/E does not support entering quoted strings in print inhibit mode; therefore your password phrase will be visible on the display. Take care to ensure that nobody can view your password phrase.

For example, to change your password phrase from “December 27, 1950” to “In 1492 Columbus sailed the ocean blue”, type:

```
PASSWORD PHRASE ('December 27, 1950' 'In 1492 Columbus sailed the ocean blue')
```

or

```
PHRASE PHRASE ('December 27, 1950' 'In 1492 Columbus sailed the ocean blue')
```

The password interval (that is, the time allowed before you are required to change your password again) also applies to the password phrase. For a description of how to change the password interval, see “Changing your password” on page 43. You can use either the PASSWORD or PHRASE command. For example, to change your password interval to 15 days, enter either of the following commands:

```
PASSWORD INTERVAL(15)
```

or

```
PHRASE INTERVAL(15)
```

At the end of 15 days, RACF requires you to change your current password phrase.

Synchronizing your passwords and password phrases

To synchronize your passwords and password phrases (that is, keep your passwords and password phrases automatically synchronized for two or more user IDs on the same system or on different systems), first you must establish peer user ID associations with password synchronization among the user IDs. Then, whenever you change the password or password phrase on one of the associated user IDs, RACF automatically communicates the new password or password phrase

Changing your system definitions

to the RACF databases of the other user IDs. For more information about defining associations for your user ID, see “User ID associations” on page 51.

An installation can also maintain the synchronization of user passwords and password phrases between the same user IDs on different nodes by using automatic password direction. See “Automatic password direction” on page 46 for additional information.

Notes:

1. User IDs do not have to have the same password or password phrase to request an association. Passwords and password phrases are synchronized automatically when either of the associated user IDs changes a password or password phrase after the peer association with password synchronization has been established.

2. Password and password phrase changes are not repropagated. For example:

User1 has an established peer user ID association with password synchronization enabled with User2, but not with User3.

User2 has an established peer user ID association with password synchronization enabled with User1 and an established peer user ID association with password synchronization enabled with User3.

If User1 changes his or her password, the new password is propagated to User2. Even though User2 has an established peer user ID association with password synchronization enabled with User3, the new password from User1 is not propagated to User3.

But, if User2 changes his or her password, the new password is propagated to both User1 and User3. This occurs because User2 has an established peer ID association with password synchronization enabled with User1 and with User3.

Automatic password direction

Installations using automatic command direction can optionally use automatic password direction to maintain the synchronization of user passwords and password phrases between the same user IDs on different nodes. Automatic password direction does not require user ID associations. Instead, automatic password direction assumes that the same user IDs on different nodes belong to the same user.

For example, suppose your installation is using automatic password direction and you have the user ID CLAIRE on three different nodes: NODE1, NODE2, and NODE3. When you change your password on NODE1, a password synchronization request is automatically directed to be processed for CLAIRE on NODE2 and CLAIRE on NODE3. You will receive a TSO SEND message on NODE1 telling you whether the password synchronization request completed successfully or unsuccessfully.

In addition, depending on how automatic password direction is set up at your installation, the output from the password synchronization request is either discarded, sent to an administrator, or returned to you and appended in your RRSFLIST user data set. If automatic password direction is set up at your installation so that you receive this output and you do not have an RRSFLIST user data set, RACF allocates one and adds the results. The RRSFLIST data set name is *'prefix.userid.RRSFLIST'*, where *prefix* is your TSO prefix at the time you changed your password. If *prefix* matches *userid* or if you specified PROFILE NOPREFIX via the TSO PROFILE command, the data set name used is *'userid.RRSFLIST'*.

You are responsible for maintaining this data set. If your data set becomes full, the output is transmitted to your user ID. In order for RACF to append to your RRSFLIST user data set again, you must edit and delete some of the returned output in this data set.

Notes:

1. If your installation is using automatic password direction, do not establish peer user ID associations with password synchronization enabled between the same user IDs across multiple RRSF nodes. Doing so causes duplicate password synchronization requests. If you are not sure whether your installation is using automatic password direction, contact your RACF security administrator.
2. You can use peer user ID associations with password synchronization enabled between user IDs that are not the same in environments with automatic password direction, because automatic password direction only synchronizes passwords and password phrases between the same user IDs on multiple RRSF nodes.
3. Password synchronization and automatic password direction only synchronize passwords and password phrases for user IDs that are not revoked on the target system.

RRSF password synchronization requests run asynchronously; that is, the command issuer does not wait until the command completes processing, and results and output from the commands are returned as specified by the SET AUTOPWD command.

Figure 45 shows the format of output produced by automatic password direction. The format of the output is the same for both your RRSFLIST data set and for the output transmitted when your data set is full.

```
=====
Password synchronization request issued at 15:03:58 on 02/28/98 was
processed at NODE2.TSOUSER on 02/28/98 at 15:04:00

Request was propagated by automatic direction from NODE1.TSOUSER

REQUEST ISSUED: From user TSOUSER at NODE1

REQUEST OUTPUT:
IRRC013I Password synchronized successfully for TSOUSER at NODE2 and
TSOUSER at NODE1.
=====
```

Figure 45. Automatic password direction: sample output

Logging on to TSO/E with a group other than your default group

Note: Some other applications also allow you to specify a group. This information applies only to TSO/E.

As a RACF user, you belong to a default group. You are automatically connected to that group when you log on to TSO/E. However, you can be defined to more than one group. If you need the resources of another group, your security administrator can give you authority to log on to that other group. For example, a particular group can use a data set containing a report that is critical to a presentation you are preparing. You need the information, so you log on to the group that has access to it.

Changing your system definitions

To log on to a group other than your default group:

Note

In most cases this procedure is needed only if your installation does not have list-of-groups processing in effect. However, in some cases it might be necessary even with list-of-groups in effect, depending on how your administrator has protected the system resources. Ask your security administrator if this procedure is necessary.

If you belong to more than one group, and have no trouble accessing information belonging to the various groups, you do not need to use this procedure.

1. Determine what groups you belong to.
You must belong to a group before you can log on to it. If you know that you belong to the group you need, proceed with Step 2. If you do not know whether you belong to the group you need, use the LISTUSER command, as described in “Finding out how you are defined to RACF” on page 16, to see a list of the groups you belong to.
2. Log on to a group other than your default group.
Enter the group name you want to log on to in the **Group Ident** field of the logon panel. Figure 46 shows a user logging on to group ABC123.

```
----- TSO/E LOGON -----  
  
Enter LOGON parameters below:          RACF LOGON parameters:  
Userid   ==> CLAIRe                    SECLABEL   ==>  
Password ==> _                          New Password ==>  
Procedure ==> PROC01                     Group Ident ==> ABC123  
Acct Nbr ==> 123199  
Size     ==>  
Perform  ==>  
Command  ==>  
  
Enter an 'S' before each option desired below:  
-Nomail      -Nonotice      -Reconnect      -OIDcard  
  
PF1/PF13 ==> Help   PF3/PF15 ==> Logoff   PA1 ==> Attention   PA2 ==> Reshow  
You may request specific help information by entering a '?' in any entry field
```

Figure 46. Logging on to another group

Logging on with a security label other than your default security label

Your installation can define its own security classifications. These classifications are security levels, security categories, and security labels. A security level is a name for a numeric security classification indicator. For example, a security level could be SECRET. A security category is a name corresponding to a department or area within an organization with similar security requirements. For example, an employee in the payroll department can be in the security category PAYROLL.

A security label is used to represent the association between a particular security level and a set of zero or more security categories. For example, the security categories PAYROLL and PERSONNEL can both be associated with the security level SECRET by the security label PPSECR.

If your installation uses security classifications, RACF stores the security classifications for each user and each data set in user and data set profiles. When you request access to a data set, RACF checks your user profile and the data set profile to see if your security label is equal to or greater than the security label of the data set. RACF denies you access if you do not have the appropriate level.

Your security administrator defines a default security label for you. However you might be able to log on with a different security label if you have been authorized. This alternate security label allows you access to resources that have the same security label.

Note: If you want to log on with a security label, your installation must have the security label class (SECLABEL) active. Check with your security administrator.

1. Determine what security labels you have authority to use.

You must first have authority to a security label before you can log on with it. If you know what security label you need, proceed with Step 2.

If you do not know whether you can use a particular security label, RACF can give you a list of all the profiles in the SECLABEL class you are authorized to use.

To see this list, log on with your default security label and enter the following command:

```
SEARCH CLASS(SECLABEL)
```

The profile names listed are the security labels you are authorized to use.

```
LOGOFF
```

2. Log on using a security label other than your default security label.
Enter the security label you want to log on with in the SECLABEL field of the logon panel. Figure 47 on page 50 shows a user logging on with security label SECRET.

Changing your system definitions

```
----- TSO/E LOGON -----  
  
Enter LOGON parameters below:                RACF LOGON parameters:  
Userid   ==> CLAIRE                          SECLABEL   ==> SECRET  
Password ==> _                               New Password ==>  
Procedure ==> PROC01                         Group Ident ==>  
Acct Nbr ==> 123199  
Size     ==>  
Perform  ==>  
Command  ==>  
  
Enter an 'S' before each option desired below:  
-Nomail      -Nonotice    -Reconnect    -OIDcard  
  
PF1/PF13 ==> Help   PF3/PF15 ==> Logoff  PA1 ==> Attention  PA2 ==> Reshow  
You may request specific help information by entering a '?' in any entry field
```

Figure 47. Logging on with another security label

Once you log on with a different security label, that new security label is associated with your user ID until you change it. The new security label appears in the SECLABEL field of the logon panel the next time you log on. If you blank out this field, and if the TERMINAL class is active and the profile covering your terminal has a security label, the system assigns the terminal's security label to your TSO session. If the terminal does not have a security label, the system assigns your default security label to your TSO session. In both of these cases, the SECLABEL field on the logon panel remains blank.

Allowing another user to submit your jobs

You can authorize another user to submit jobs on your behalf. This user is called a *surrogate user*. You are the *execution user*. For example, if you need certain jobs submitted while you are on vacation, you can authorize a surrogate user to submit these jobs for you. You do not have to give the surrogate user access to the data sets the jobs use. You also do not have to give the surrogate user your password, although the jobs will execute under your user ID.

The use of surrogate users might not be allowed on some systems, or might have to be set up by the security administrator. Contact your security administrator to find out if surrogate users are allowed on your system and if you can set them up.

Attention

Do not allow another user to act as surrogate user for you *unless the surrogate user can be trusted as much as you are trusted*. This is because the surrogate user can do anything you can do (unless the surrogate user lacks access to a security label that protects a resource). For example, the surrogate user can submit a job to copy, alter, or delete your data.

To give a surrogate user authority to submit a job for you:

1. If security labels are used on your system, determine if the surrogate user has access to the security label the job will run under.

To determine if the surrogate user has access to the security label under which the job will run, ask the surrogate user to enter the following command:

```
SEARCH CLASS(SECLABEL)
```

If the security label under which the job will run does not appear in the list of security labels, the surrogate user cannot run the job for you. Ask your RACF security administrator for assistance or find a different surrogate user who does have the correct security label authority.

2. Determine if the surrogate user has authority to submit your job.

Determine if a profile called *your-userid.SUBMIT* exists and if it has an access list identifying the surrogate user with at least READ authority.

To list information about the *your-userid.SUBMIT* profile, enter the following command:

```
RLIST SURROGAT your-userid.SUBMIT AUTHUSER
```

If the profile exists, RACF lists information about the profile, including the access list. If the surrogate user is on the access list and has an access authority of at least READ, proceed to Step 3.

If the profile does not exist, RACF gives you an error message. You can create the profile yourself if you have class authority to the SURROGAT class. When the SECLABEL class is active, both you and the surrogate user must have authority to the security label of your job. If you need help creating the SURROGAT class profile, ask your security administrator.

3. Give the surrogate user authority to submit your job.

To give the surrogate user READ access to the *your-userid.SUBMIT* profile, enter the following command:

```
PERMIT your-userid.SUBMIT CLASS(SURROGAT)  
ID(surrogate-userid) ACCESS(READ)
```

See “When data set profile changes take effect” on page 89 to find out when the surrogate user will have the necessary access authority after you enter this command. Proceed to Step 4.

4. Make sure the surrogate user has access to the data set containing the job control language (JCL) for that job.

The user does not necessarily need access to the data sets the job uses, only to the data set containing the JCL. You can give the surrogate user this access by either sending a copy of the data set or giving the surrogate user READ access to it. For more information about giving someone READ access to a data set, see “Permitting an individual or a group to use a data set” on page 74.

Note: Make sure the USER parameter on the JOB statement in the JCL is present and specifies your user ID. For surrogate processing to be performed, the PASSWORD parameter must not be specified.

5. To revoke a surrogate user’s authority to submit your jobs, enter the following command; the user will no longer be a surrogate user who can submit your jobs:

```
PERMIT your-userid.SUBMIT CLASS(SURROGAT)  
ID(surrogate-userid) DELETE
```

User ID associations

A RACF user ID can have multiple user ID associations, that is, associations defined between your user ID and another user ID. There are two types of user ID association: peer and managed.

Changing your system definitions

With a peer user ID association, either user ID in the association can direct allowed RACF commands to run under the authority of the other user ID. See “Directing commands” on page 10 for information on directing commands. A peer user ID association can be defined with or without password synchronization, and can be deleted by either user.

With a managed user ID association, the managing user ID in the association can direct allowed RACF commands to run under the authority of the managed user ID. The managed user ID cannot direct RACF commands to run under the authority of the managing user ID. See “Directing commands” on page 10 for information on directing commands. A managed user ID association cannot be defined with password synchronization, but can be deleted by either user.

Note: Your RACF security administrator determines whether you can define user ID associations. If you are not sure, contact your RACF security administrator. Also, an authorized user can establish user ID associations between your user ID and another user ID provided that user has the authority to do so. You receive a notification message to indicate any such activity.

Defining a peer user ID association with password synchronization

To see the user ID associations that are already established for your user ID or are pending approval, see “Finding out what user ID associations are defined for you” on page 39.

To define a peer user ID association with password synchronization, enter the RACLINK command with the DEFINE keyword as follows:

```
RACLINK DEFINE(target-node.target-userid  
[/target-userid-password]) PEER(PWSYNC)
```

For example, to define a peer user ID association between your two user IDs, JOHN on MVS01 and JDOE on MVS03, enter the following command from your user ID JOHN on MVS01:

```
RACLINK DEFINE(MVS03.JDOE/password-of-JDOE) PEER(PWSYNC)
```

Because you specified the password for your JDOE user ID in the preceding example, the user ID association between your user IDs is established and approved without requiring you to logon to your JDOE user ID to issue a subsequent RACLINK APPROVE command.

If you didn't specify the password for JDOE on MVS03 in the preceding example, the user ID association would be pending until JDOE on MVS03 issued a subsequent RACLINK APPROVE command.

Note: User IDs do not need the same password or password phrase to request an association. Passwords and password phrases are synchronized automatically when either of the associated user IDs changes a password or password phrase after the peer association with password synchronization has been established.

Defining a peer user ID association without password synchronization

To see the user ID associations that are already established for your user ID or are pending your approval, see “Finding out what user ID associations are defined for you” on page 39.

To define a peer user ID association without password synchronization, enter the RACLINK command with the DEFINE keyword as follows:

```
RACLINK DEFINE(target-node.target-userid  
[/target-userid-password]) PEER(NOPWSYNC)
```

For example, to define a peer user ID association between your user ID JOHN on MVS01 and a co-worker's user ID SMITH on MVS01, enter the following command from your user ID JOHN on MVS01:

```
RACLINK DEFINE(MVS01.SMITH/password-of-SMITH) PEER(NOPWSYNC)
```

Because you specified the password of your co-worker's user ID SMITH on MVS01 in the preceding example, the user ID association between the two user IDs is established and approved without requiring the owner of the SMITH user ID on MVS01 to issue a subsequent RACLINK APPROVE command.

If you didn't specify the password for SMITH on MVS01 in the preceding example, the user ID association would be pending until SMITH on MVS01 issued a subsequent RACLINK APPROVE command.

Defining a managed user ID association

To see the user ID associations that are already established for your user ID or are pending your approval, see "Finding out what user ID associations are defined for you" on page 39.

To define a managed user ID association, enter the RACLINK command with the DEFINE keyword as follows:

```
RACLINK DEFINE(target-node.target-userid  
[/target-userid-password]) MANAGED
```

The user ID that issues this RACLINK command manages the target user ID.

For example, suppose you want your user ID JOHN on MVS01 to manage another user ID: OPER2 on MVS03. To define a managed user ID association between JOHN and OPER2, enter the following command from your user ID JOHN on MVS01:

```
RACLINK DEFINE(MVS03.OPER2) MANAGED
```

Because user ID JOHN did not enter the password of OPER2 to approve the user ID association between JOHN and OPER2, OPER2 will receive a notification message that this user ID association is in the process of being established. The association will be pending until OPER2 issues a subsequent RACLINK APPROVE command.

Approving user ID associations

To see the user ID associations that are already established for your user ID or are pending your approval, see "Finding out what user ID associations are defined for you" on page 39.

To approve a pending user ID association, enter the RACLINK command with the APPROVE keyword as follows:

```
RACLINK APPROVE(node.userid)
```

To approve the association in the previous example, OPER2 on MVS03 would issue the following command:

Changing your system definitions

```
RACLINK APPROVE(MVS01.JOHN)
```

Deleting user ID associations

To see the user ID associations that are already established for your user ID or are pending your approval, see “Finding out what user ID associations are defined for you” on page 39.

To reject a pending association or to delete an existing association, enter the RACLINK command with the UNDEFINE keyword as follows:

```
RACLINK UNDEFINE(node.userid)
```

To reject the association in the previous example, OPER2 on MVS03 would issue the following command:

```
RACLINK UNDEFINE(MVS01.JOHN)
```

Chapter 6. Protecting a data set

RACF can protect your data sets from other users by controlling who has authority to access them and at what authority level they can do so. You can use RACF to protect data sets by creating profiles for them. When you attempt to use a data set, RACF checks your user profile as well as the data set profile to decide whether to allow you to use it.

A data set profile contains the following:

- The data set name.
- The data set owner.
- The access list, which is a list of specific users and groups who can use a data set and how they can use it.
- The universal access authority (UACC), which is the default level of access authority allowed for all users or groups not specified in the access list.
- Auditing information. RACF can audit the use of each data set. The audit can be general or specific. For example, you can set up a resource profile for your data set to audit every attempt to use that data set. Or, you can define the profile to audit only the attempts to update the data set.

You can protect a data set by identifying specific users or groups with the access you want them to have in the access list. You can give all other RACF-defined users a certain access. Just put ID(*) in the access list with the access authority you want them to have. All other users are allowed the access you specify as the universal access authority (UACC). The access authorities you can specify are: NONE, READ, UPDATE, CONTROL, ALTER, and EXECUTE. See “Creating a discrete profile to protect a data set” on page 57 for more information about each. To protect a data set most effectively, you should initially specify a UACC of NONE and selectively give certain users specific access authority to the data set.

You can use RACF to protect your data sets by doing the tasks described in this chapter.

Choosing between discrete and generic profiles

Data set profiles contain a description of a data set, including the authorized users and the access authority of each user. They can either be discrete or generic. Check with your security administrator to find out your installation's policy on whether to use discrete or generic profiles. Most security administrators prefer to use generic profiles.

A *discrete* profile protects a single data set that has unique security requirements. The name of a discrete profile must exactly match the name of the data set it protects. The data set SMITH.PAYROLL.INFO would be protected by the discrete data set profile SMITH.PAYROLL.INFO.

You would choose a discrete profile to protect one data set with unique security requirements.

To create a discrete profile, see “Creating a discrete profile to protect a data set” on page 57.

Protecting data sets

A *generic* profile protects several data sets that have a similar naming structure and security requirements. The name of a generic data set profile need not exactly match the names of the data sets it protects. Rather, it can contain generic characters that match any other characters. You can protect many data sets with similar characteristics with a generic profile. Two advantages of a generic profile are:

- Data sets protected by a generic profile do not have to be individually defined to RACF
- The generic profile protects all copies of the data sets on all volumes in all locations in the system.

If a data set is protected by both a generic profile and a discrete profile, the discrete profile sets the level of protection for the data set. If a data set is protected by multiple generic profiles, the most specific generic profile sets the level of protection for the data set.

In general, given two profiles that match a data set, you can find the more specific one by comparing the profile name from left to right. Where they differ, a non-generic character is more specific than a generic character. In comparing generics, a % is more specific than an *, and an * is more specific than **. Another way to determine the most specific is with the SEARCH command, as there are some rare exceptions to the general rule. SEARCH always lists the profiles in the order of the most specific to the least specific.

A generic profile might already exist to protect your data set. However, that profile might not provide the exact protection you want. In this case, you can create a more specific generic profile or a discrete profile for the data set.

You would choose a generic profile for one of the following reasons:

- To protect more than one data set with the same security requirements. The data sets protected by a generic profile must have some identical characters in their names. The profile name contains one or more generic characters (*, **, or %).
- If you have a single data set that might be deleted, then re-created, and you want the protection to remain the same, you can create a *fully-qualified* generic profile. The name of a fully-qualified generic profile matches the name of the data set it protects. Unlike a discrete profile, a fully-qualified generic profile is not deleted when the data set itself is deleted. Also, with a fully-qualified generic profile, you can have multiple data sets with the same name all protected with the same profile.

To create a generic profile, see “Creating a generic profile to protect a data set” on page 59.

Notes:

1. Deleting a data set that is protected with a discrete profile causes RACF to delete the data set profile from the RACF database.
2. If your installation is using automatic direction of application updates, you might receive output from an automatic direction of application update request when you do any of the following:
 - Define a data set when you have the ADSP attribute
 - Delete a data set that is protected with a discrete profile
 - Rename a data set that is protected with a discrete profile

See “Automatic direction of application updates” on page 90 for more information.

3. All the members of a partitioned data set (PDS) are protected by the profile that protects the data set. The members of a PDS cannot have different protection. If different protection is desired, those members should be moved to a different PDS.
4. All the components of a VSAM data set are protected by the profile that protects the cluster name. You do not need to create profiles that protect the index and data components of a cluster.
5. For a generic profile, unit and volume information, if specified, is ignored because the data sets that are protected under the generic profile can be on many different volumes.

Creating a discrete profile to protect a data set

Create a discrete profile to protect a data set if you have a single data set with unique security requirements. To create a discrete profile:

1. Decide which RACF protections to use:

There are different options you can use depending on how much protection you want.

Note: To give specific authority to a certain user you could include that user on the access list for that data set. To do that see “Permitting an individual or a group to use a data set” on page 74.

The following options provide different degrees of general protection for your data set:

- UACC (universal access authority).

Universal access authority specifies the authority any user not on the access list has to use the data set. The UACC can be one of the following:

NONE Does not allow users to access the data set.

Attention

Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected data set can create a copy of it. As owner of the copied data set, that user has control of the security characteristics of the copied data set, and can downgrade it. For this reason, you might want to initially assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See “Permitting an individual or a group to use a data set” on page 74 for information on how to permit selected users or groups to access a data set.)

READ Allows users to access the data set for reading only. (Note that users who can read the data set can copy or print it.)

UPDATE

Allows users to read from, copy from, or write to the data set. UPDATE does not, however, authorize a user to delete, rename, move, or scratch the data set.

CONTROL

For VSAM data sets, CONTROL is equivalent to the VSAM CONTROL password; that is, it allows users to perform

Protecting data sets

control-interval access (access to individual VSAM data blocks), and to retrieve, update, insert, or delete records in the specified data set.

For non-VSAM data sets, CONTROL is equivalent to UPDATE.

ALTER

ALTER allows users to read, update, delete, rename, move, or scratch the data set.

When specified in a discrete profile, ALTER allows users to read, alter, and delete the profile itself *including the access list*. However, ALTER does not allow users to change the owner of the profile.

When specified in a generic profile, ALTER gives users *no* authority over the profile itself.

When specified in a generic profile, ALTER allows users to create new data sets that are covered by that profile.

EXECUTE

For a private load library, EXECUTE allows users to load and execute, but not read or copy, programs (load modules) in the library.

Note: In order to specify EXECUTE for a private load library, you must ask for assistance from your RACF security administrator.

- NOTIFY user ID.

The NOTIFY user ID is sent a message whenever someone tries to use a data set, and RACF denies the access.

For example, if your user ID is specified on the NOTIFY keyword, and a user with READ access attempts to update a protected data set, you receive a message identifying the user who attempted the access and what kind of access was attempted.

Note: If you do not specify a user ID on the NOTIFY keyword, your user ID is the default NOTIFY user ID.

- Erase-on-scratch.

You might want to specify that the data set protected by this profile be physically erased when the data set is deleted (scratched) or released for re-use. Erasing the data set means overwriting all allocated extents with binary zeros. To use erase-on-scratch, specify the ERASE operand on the ADDSD command.

- WARNING option.

Specifying WARNING allows *unauthorized* users to access a data set. RACF issues a warning message to the user requesting access, then allows the access.

Attention

WARNING is generally used only during a transition period when RACF is first installed. If you use WARNING, it is equivalent to no protection.

- Your installation might have other security requirements for protecting data, including audit type, level, and security label. See your RACF security administrator for specific information.

2. Create the profile for the data set.

To create a discrete profile for a cataloged data set, enter the ADDSD command as follows:

```
ADDSD 'dataset-name' UACC(access-authority)
```

Note: A cataloged data set is one that is represented in an index in the system catalog.

For example, to create a discrete profile for data set SMITH.PROJ.ONE, enter the following command:

```
ADDSD 'SMITH.PROJ.ONE' UACC(NONE)
```

To create a discrete profile for a data set that is not cataloged, you must specify the unit type and volume serial number of the data set. Enter the ADDSD command as follows:

```
ADDSD 'dataset-name' UNIT(type) VOLUME(volume-serial) +
      UACC(access-authority)
```

For example, to create a discrete profile for data set SMITH.PROJ.ONE, enter the following command:

```
ADDSD 'SMITH.PROJ.ONE' UNIT(3380) VOLUME(ABC123) +
      UACC(NONE)
```

To create a discrete profile with a NOTIFY user ID, enter the ADDSD command as follows:

```
ADDSD 'data-set-name' UACC(access-authority) NOTIFY(userid)
```

For example, if your user ID is SMITH, and you want to be notified when RACF denies access to data set SMITH.PROJ.ONE, enter the following command:

```
ADDSD 'SMITH.PROJ.ONE' UACC(NONE) NOTIFY
```

If your user ID is SMITH, and you want JONES to be notified when RACF denies access to data set SMITH.PROJ.ONE, enter the following command:

```
ADDSD 'SMITH.PROJ.ONE' UACC(NONE) NOTIFY(JONES)
```

To create a discrete profile for a VSAM data set, you can use the VSAM cluster name on the ADDSD command. The following example illustrates how this is done.

SMITH has created a VSAM cluster using the following command:

```
DEFINE CLUSTER(NAME('SMITH.SAMPLE') VOLUMES(VSAM02) ) +
      INDEX(NAME('SMITH.SAMPLEI') TRACKS(1 1) ) +
      DATA(NAME('SMITH.SAMPLED') CYLINDERS(1 1) KEYS(128 0) +
      CONTROLINTERVALSIZE(X'1000') )
```

SMITH can protect this cluster with a profile named 'SMITH.SAMPLE', as follows:

```
ADDSD 'SMITH.SAMPLE' UACC(NONE) NOTIFY
```

Creating a generic profile to protect a data set

Create a generic profile if you have several data sets that have the same security requirements and that have some identical characters in their names. To create a generic profile:

1. Decide how to specify the profile name.

To define a generic profile you either include one or more generic characters (% , * , **) in the profile name or you specify the profile as a generic profile.

You can use the following generic characters when naming generic profiles:

% (percent sign)

A percent sign matches one and only one character. For example, a generic data set profile named AB.CD.% protects data sets named AB.CD.E and AB.CD.F, but not AB.CD.EF.

Protecting data sets

* (asterisk)

An asterisk used as a qualifier in the middle of a profile name (for example, ABC.*.DEF) matches one and only one qualifier.

An asterisk used as a character at the end of a qualifier in the middle of a profile name (for example, ABC.DE*.FGH) matches zero or more characters until the end of the qualifier.

An asterisk used at the end of a profile name has different meanings depending upon whether enhanced generic naming (EGN) is active.

- When enhanced generic naming is not active:
 - An asterisk used as a character at the end of a profile name (for example, ABC.DEF*) matches zero or more characters until the end of the name, zero or more qualifiers until the end of the name, or both.
 - An asterisk used as a qualifier at the end of a profile name (for example, ABC.DEF.*) matches one or more qualifiers until the end of the name.
- When enhanced generic naming is active:
 - An asterisk used as a character at the end of a profile name (for example, ABC.DEF*) matches zero or more characters until the end of the qualifier.
 - An asterisk used as a qualifier at the end of a profile name (for example, ABC.DEF.*) matches one and only one qualifier.

To find out whether EGN is active at your installation, ask your security administrator.

** (double asterisk)

A double asterisk matches zero or more qualifiers. For example, a generic data set profile named AB.CD.** protects data sets named AB.CD, AB.CD.EF, and AB.CD.EF.XYZ.

Note: The double asterisk (**) is allowed with the DATASET class if enhanced generic naming (EGN) is active. Ask your security administrator if EGN is active at your installation.

If a data set matches more than one generic profile, the most specific profile sets the level of protection for the data set. For example, assume there are two generic profiles, USERID.** and USERID.GAMES.*. A data set named USERID.GAMES.INDOOR would be protected by profile USERID.GAMES.*. Profile USERID.** would not protect the data set.

To create a generic profile for your user data set, the high-level qualifier must be your user ID. For example, for user ASMITH to protect data set ASMITH.PROJ.ONE, ASMITH must specify a profile name beginning with ASMITH (such as ASMITH.PROJ.* or ASMITH.PROJ.**).

You create a generic profile in the same manner as a discrete profile, except that you include one or more generic characters (% or *) in the profile name or you include the GENERIC keyword on the ADDSD command.

See “Profile names for data sets” on page 86 for information about generic profile names with enhanced generic naming active and inactive.

How to specify the generic characters depends on whether your installation uses *enhanced generic naming*. Ask your RACF security administrator if enhanced generic naming is active.

If enhanced generic naming is active, see “Generic profile rules when enhanced generic naming is active” on page 88 for a description of how to specify generic characters in profile names.

If enhanced generic naming is *not* active, see “Generic profile rules when enhanced generic naming is inactive” on page 86 for a description of how to specify generic characters in profile names.

Note: Profiles created *before* an installation converts to enhanced generic naming are *not* affected by the conversion. Profiles created *after* the installation converts to enhanced generic naming are governed by the new rules.

2. Decide which RACF protections to use.

There are different options you can use depending on how much protection you want.

Note: To give specific authority to a certain user you could include that user on the access list for that data set. To do that see “Permitting an individual or a group to use a data set” on page 74.

The following options provide different degrees of general protection for your data set:

- **UACC** (universal access authority)

Universal access authority specifies the authority any user that is not on the access list has to use the data set. The UACC can be one of the following:

NONE Does not allow users to access the data set.

Attention

Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected data set can create a copy of it. As owner of the copied data set, that user has control of the security characteristics of the copied data set, and can downgrade it. For this reason, you might want to initially assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See “Permitting an individual or a group to use a data set” on page 74 for information on how to permit selected users or groups to access a data set.)

READ Allows users to access the data set for reading only. (Note that users who can read the data set can copy or print it.)

UPDATE

Allows users to read from, copy from, or write to the data set. UPDATE does not, however, authorize a user to delete, rename, move, or scratch the data set.

CONTROL

For VSAM data sets, CONTROL is equivalent to the VSAM CONTROL password; that is, it allows users to perform control-interval access (access to individual VSAM data blocks), and to retrieve, update, insert, or delete records in the specified data set.

For non-VSAM data sets, CONTROL is equivalent to UPDATE.

ALTER

ALTER allows users to read, update, delete, rename, move, or scratch the data set.

Protecting data sets

When specified in a discrete profile, ALTER allows users to read, alter, and delete the profile itself *including the access list*. However, ALTER does not allow users to change the owner of the profile.

When specified in a generic profile, ALTER gives users *no* authority over the profile itself.

When specified in a generic profile, ALTER allows users to create new data sets that are covered by that profile.

EXECUTE

For a private load library, EXECUTE allows users to load and execute, but not read or copy, programs (load modules) in the library.

Note: To specify EXECUTE for a private load library, you must ask for assistance from your RACF security administrator.

Note: If you do not specify UACC, the system uses the value specified in the UACC field in your current connect group. (For more information, see “Finding out what authority you have as a member of a group” on page 20.)

- NOTIFY user ID.

The NOTIFY user ID is sent a message whenever someone tries to use a data set, and RACF denies the access.

For example, if your user ID is specified on the NOTIFY keyword, and a user with READ access attempts to update a protected data set, you receive a message identifying the user who attempted the access and what kind of access was attempted.

Note: If you do not specify a user ID on the NOTIFY keyword, your user ID is the default NOTIFY user ID.

- Erase-on-scratch.

If allowed by your installation, you can specify that a data set protected by this profile be physically erased when the data set is deleted (scratched) or released for re-use. Erasing the data set means overwriting all allocated extents with binary zeros. To use erase-on-scratch, specify the ERASE operand on the ADDSD command.

Note: Only the data set that is deleted is erased. For example, the profile SMITH.SAMPLE*.DATA protects data sets SMITH.SAMPLE1.DATA and SMITH.SAMPLE2.DATA. If SMITH.SAMPLE1.DATA is deleted, only SMITH.SAMPLE1.DATA is erased. SMITH.SAMPLE2.DATA is not affected.

- WARNING option.

Specifying WARNING allows *unauthorized* users to access a data set. RACF issues a warning message to the user requesting access, then allows the access.

Attention

WARNING is generally used only during a transition period when RACF is first installed. If you use WARNING, it is equivalent to no protection.

Your installation might have other security requirements for protecting data, including audit type, level, and security label. See your RACF security administrator for specific information.

3. Create the profile.

To create a generic profile, enter the ADDSD command as follows:

```
ADDSD 'profile-name-with-generic-character' UACC(access-authority)
```

To create a fully-qualified generic profile, enter the ADDSD command as follows:

```
ADDSD 'profile-name' UACC(access-authority) GENERIC
```

Note: Changes to the profile will take effect for other users when they log off and log on again. For additional information, see “When data set profile changes take effect” on page 89.

Example 1. A generic profile for all data sets not otherwise protected

You can create a generic profile to protect all of your data sets that are not protected by more specific profiles. To do this, enter one of the following commands:

- If your system has enhanced generic naming:

```
ADDSD 'prefix.**' UACC(NONE)
```

- If your system does not have enhanced generic naming:

```
ADDSD 'prefix.*' UACC(NONE)
```

where *prefix* is your user ID. The profile created allows a universal access authority (UACC) of NONE.

Example 2. A generic profile for data sets whose last qualifier is TESTDATA

You can create a generic profile to protect all of your data sets that have three qualifiers whose last qualifier is TESTDATA. To do this, enter the following command:

```
ADDSD 'prefix.*.TESTDATA' UACC(NONE)
```

where *prefix* is your user ID. The profile created allows a universal access authority (UACC) of NONE. You can permit or deny specific users or groups access to these data sets. For more information, see “Permitting an individual or a group to use a data set” on page 74 or “Denying an individual or a group use of a data set” on page 75.

Example 3. A generic profile for group data sets

You can create a generic profile to protect all of a group’s data sets that are not protected by more specific profiles. To do this, enter one of the following commands:

- If your system has enhanced generic naming:

```
ADDSD 'groupname.**' UACC(NONE)
```

- If your system does not have enhanced generic naming:

```
ADDSD 'groupname.*' UACC(NONE)
```

where *groupame* is the group name. The profile that is created allows a universal access authority (UACC) of NONE.

Example 4. A fully-qualified generic profile

You want to allow a universal access of READ to a particular listing file that you will be deleting and recreating. To do this, enter the following command:

```
ADDSD 'prefix.SAMPLE.LISTING' UACC(READ) GENERIC
```

where *prefix* is your user ID. The profile created allows a universal access authority (UACC) of READ.

Finding out how a data set is protected

If you are the owner of a data set, you might want to determine what protection the data set has. For example, you might want to find out what users and groups can access the data set.

Note: Contact your security administrator if any problems occur with your data set protection.

To see how a data set is protected:

1. Determine if a discrete profile protects the data set by issuing the LISTDSD command as follows:

```
LISTDSD DATASET('dataset-name') ALL
```

You will see one of the following on your screen:

- A listing for that profile, if the data set is protected by a discrete profile.
- A listing for the generic profile, if the data set is not protected by a discrete profile but is protected by a fully-qualified generic profile, and generic profile command processing is active. (A generic profile is identified by a “G” in parentheses following the profile name.)
- A message stating that no profile was found, if the data set is not protected by a discrete profile.

Note: If generic profile checking is active, and you get the message that no profile was found, you must do Step 2 to check for generic profiles.

If the command succeeds, you will see a listing of the profile similar to that shown in Figure 48 on page 65.

2. Determine if the data set is protected by a generic profile by entering the LISTDSD command with the GENERIC operand as follows:

```
LISTDSD DATASET('dataset-name') ALL GENERIC
```

You will see one of the following on your screen:

- A listing for that profile, if the data set is protected by a fully-qualified generic profile.
- A listing for the most specific generic profile that protects the data set, if the data set is not protected by a fully-qualified generic profile but is protected by a generic profile.
- A message stating that no profile was found, if the data set is not protected by a generic profile.

If the command succeeds, you will see a listing of the profile, similar to that shown in Figure 48 on page 65.

If the command indicates that a profile is not found, protect the data set with a discrete or generic profile. See “Creating a discrete profile to protect a data set” on page 57 or “Creating a generic profile to protect a data set” on page 59 for more information. If the command fails, contact your RACF security administrator.

```

INFORMATION FOR DATASET profile-name

LEVEL   OWNER           UNIVERSAL ACCESS   WARNING   ERASE
-----  -----
 00     SMITH              READ            NO        NO

AUDITING
-----
SUCCESS(UPDATE)

NOTIFY
-----
NO USER TO BE NOTIFIED

YOUR ACCESS           CREATION GROUP     DATASET TYPE
-----
  READ                DEPTD60            NON-VSAM

VOLUMES ON WHICH DATASET RESIDES           UNIT
-----
          21345                                SYSDA

INSTALLATION DATA
-----
PL/1 LINK LIBRARY

          SECURITY LEVEL
-----
NO SECURITY LEVEL

CATEGORIES
-----
NOCATEGORIES

SECLABEL
-----
NO SECLABEL

CREATION DATE   LAST REFERENCE DATE   LAST CHANGE DATE
(DAY) (YEAR)     (DAY) (YEAR)         (DAY) (YEAR)
-----
 070  95           090  98               090  98

ALTER COUNT     CONTROL COUNT     UPDATE COUNT     READ COUNT
-----
 00000          00000             00002            00000

  ID     ACCESS     ACCESS COUNT
-----
 JONES   UPDATE         00009

  ID     ACCESS     ACCESS COUNT     CLASS     ENTITY NAME
-----
NO ENTRIES IN CONDITIONAL ACCESS LIST

DFP INFORMATION

RESOWNER
-----
SMITH

```

Figure 48. LISTDSD command: sample output

Check the following fields for the most important security information about how the data set is protected:

Protecting data sets

- LEVEL field (if used at your installation)
- OWNER field
- UNIVERSAL ACCESS field
- WARNING field
- SECURITY LEVEL field (if used at your installation)
- CATEGORIES field (if used at your installation)
- SECLABEL field (if used at your installation)
- ID field and its related ACCESS and ACCESS COUNT fields
- PROGRAM field and its related ID, ACCESS, and ACCESS COUNT fields

Here are detailed descriptions of the fields appearing in the output:

INFORMATION FOR DATASET *profile-name*

This phrase appears for each data set profile listed.

Note: If the profile is a generic profile, the phrase looks like the following:

INFORMATION FOR DATASET *profile-name* (G)

LEVEL

A security classification indicator used by each individual installation. If anything other than 00 appears in this field, see your RACF security administrator for an explanation of the number.

OWNER

Each RACF-defined data set has an owner, which can be a user ID or a group. When you create a data set and then RACF-protect the data set without specifying an owner, RACF names you as the owner of the data set profile. The owner of the profile can modify the data set profile.

UNIVERSAL ACCESS

Each data set protected by RACF has a universal access authority (UACC). The UACC permits users or groups to use the data set in the manner specified in this field. In this example, the UACC is READ. Anyone can read this data set. (The only exception is if the user or group is specifically named in the access list with ACCESS of NONE.)

WARNING

If this field contains YES, RACF permits a user to access this resource *even though his or her access authority is insufficient*. RACF issues a warning message *to the user who is attempting access*; you are notified only if your user ID is the NOTIFY user ID.

If this field contains NO, RACF denies access to users with insufficient authority to access this resource.

ERASE

If this field contains YES, and erase-on-scratch is in effect on your system, data management physically erases the DASD data set extents when the data set is deleted. If this field contains NO, data management will not erase DASD data set extents when the data set is deleted.

Exception

Your installation could specify erase-on-scratch for all data sets that have a security level equal to or greater than the security level specified by the installation. If this data set's security level is equal to or greater than the security level specified by the installation, this data set will be erased even if the ERASE field in the profile contains NO.

AUDITING

The type of access attempts that are recorded. In this example, the AUDITING is SUCCESS(UPDATE). RACF records all successful attempts to update the data set.

NOTIFY

The user ID of a RACF-defined user that RACF notifies when denying access to a data set protected by this profile.

YOUR ACCESS

How you can access this data set.

If you must work with the listed data set but do not have the required authority, ask the owner (OWNER field) to issue a PERMIT command to give you access to the data set.

CREATION GROUP

The group under which the profile was created.

DATASET TYPE

The data set type. It can be either VSAM, NON-VSAM, MODEL, or TAPE.

VOLUME ON WHICH THE DATASET RESIDES

The volume on which a non-VSAM data set resides or the volume on which the catalog for a VSAM data set resides.

UNIT

The unit type for a non-VSAM data set.

INSTALLATION-DATA

Any information your installation keeps in this data set profile.

CREATION DATE

The date the profile was created.

SECURITY-LEVEL

Your installation can define its own security levels. This security level is a name associated with the numeric value shown in the LEVEL field earlier in this output. The security level displayed is the minimum security level you need to access a data set protected by this profile.

CATEGORIES

Your installation can define its own security categories. The names displayed are the security categories you need to access a data set protected by this profile.

SECURITY-LABEL

Your installation can define its own security labels. This security label is a name used to represent the association between a particular security level and a set of zero or more security categories. The security label displayed is the minimum security label you need to access a data set protected by this profile.

LAST REFERENCE DATE

The last time the profile was accessed.

LAST CHANGE DATE

The last time the profile was changed.

ALTER COUNT

The total number of times the data set protected by the profile was altered (not present for generic profiles).

Protecting data sets

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, this value does not change.

CONTROL COUNT

The total number of times the data set protected by the profile was successfully accessed with CONTROL authority (not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, this value does not change.

UPDATE COUNT

The total number of times the data set protected by the profile was successfully accessed with UPDATE authority (not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, this value does not change.

READ COUNT

The total number of times the data set protected by the profile was successfully accessed with READ authority (not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, this value does not change.

ID, ACCESS, and ACCESS COUNT

These fields describe the standard access list. ID is the user ID or group name given the access authority listed in the ACCESS field. ACCESS COUNT is the number of times the user listed in the ID field accessed the data set (ACCESS COUNT is not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, this value does not change.

ID, ACCESS, ACCESS COUNT, CLASS, and ENTITY NAME

These fields refer to entries in the conditional access list. A conditional access list is an access list in the data set profile that specifies another condition which must be satisfied for a user to get the specified access authority.

The CLASS and ENTITY NAME fields describe one of the following conditions which must be satisfied before authorization to the data set is granted to the user in the ID field.

1. If CLASS is APPCPORT, the ENTITY NAME is the name of the APPC port of entry, or logical unit (LU), through which the user must enter the system.
2. If CLASS is CONSOLE, the ENTITY NAME is the name of the system console from which the request must be sent.
3. If CLASS is JESINPUT, the ENTITY NAME is the name of the JES input device through which the user must enter the system.
4. If CLASS is PROGRAM, the ENTITY NAME is the name of the program the user must be running.
5. If CLASS is TERMINAL, the ENTITY NAME is the name of the terminal through which the user must enter the system.

ACCESS is the level of access to the data set that RACF grants when the condition is satisfied.

ACCESS COUNT is the number of times the user has accessed the data set under the condition described (ACCESS COUNT is not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, the ACCESS COUNT value does not change.

DFP INFORMATION / RESOWNER

The RESOWNER field contains the user ID or group name of the owner of the resource. In this case, the resource is the data set; the owner of the data set need not be the same as the owner of the profile.

Finding out what data set profiles you have

You can have RACF list the names of the profiles you own. If you want to see what data set profiles you have:

1. Find out what data set profiles you have, by entering the SEARCH command as follows:

```
SEARCH
```

RACF lists all of your profiles that are in the DATASET class. If you do not have any DATASET profiles, RACF displays a message telling you that no entries meet the search criteria.

2. Review the list of profiles, comparing them with the names of the data sets you need to protect.

Any profile name that matches a data set name protects that data set.

Any profile name that includes generic characters (% or *) might or might not protect data sets. See “Profile names for data sets” on page 86 for information on the rules for specifying generic characters.

Deleting a data set profile

When you delete a data set profile, any data set previously protected by that profile:

- Is protected by the most specific generic profile if the profile deleted was a discrete data set profile.
- Is protected by the next most specific generic profile if the profile deleted was a generic data set profile.
- Has no RACF protection if no generic profiles exist that protect the data set, unless the security administrator has activated the PROTECTALL(FAILURES) SETROPTS option. When this option is active, the system rejects any attempt to create or access a data set that is not RACF-protected.

Attention

When you remove RACF protection from a data set, anyone (RACF-defined or not) can access, change, or delete your data set, unless the security administrator has activated the PROTECTALL(FAILURES) SETROPTS option. You can selectively “remove” protection by using the PERMIT command to permit or deny access to your data set by selected users and groups. See “Permitting an individual or a group to use a data set” on page 74 and “Denying an individual or a group use of a data set” on page 75.

To delete a data set profile:

1. Find the name of the profile that currently protects the data set. To do this, see “Finding out how a data set is protected” on page 64.
2. Remove RACF protection.

Protecting data sets

If the data set is protected by a discrete profile, or if you are removing protection from all data sets covered by a generic profile, delete the data set profile by issuing the DELDSD command as follows:

```
DELDSD 'profile-name'
```

This deletes the profile, but leaves the data set intact.

Example 1:

To remove RACF protection from data set SMITH.PROJ.ONE, which is protected by a discrete profile, type:

```
DELDSD 'SMITH.PROJ.ONE'
```

Example 2:

To remove RACF protection from data sets SMITH.FIRST.DATA, SMITH.SECOND.DATA, and SMITH.THIRD.DATA, which are protected by profile SMITH.*.DATA, enter the following command:

```
DELDSD 'SMITH.*.DATA'
```

Attention

Be careful when you delete a generic profile that you are not inadvertently removing RACF protection from a data set that should remain protected. In the previous example, RACF protection would be removed from any data set whose name matched the profile name, such as SMITH.OTHER.DATA.

To list all catalogued data sets that are protected by a profile, enter the following command:

```
LISTDSD DA(profile-name) DSNS NORACF
```

You can then check which data sets are protected by the profile before deleting it.

Note also that when you delete a discrete or generic profile, the data set might still be protected by another generic profile. In the examples above, the data sets might be protected by the profile SMITH.** (if enhanced generic naming is in effect) or the profile SMITH.* (if enhanced generic naming is not in effect). Be careful that the new protecting profile provides appropriate protection.

Example 3:

To “remove protection” from a data set without deleting a profile or renaming the data set, protect the data set with a profile that has UACC(ALTER) and no names in the access list.

Note: Other security characteristics of the profile, such as LEVEL and SECLEVEL, might still be required by your installation and defined in the profile.

Example 4:

If data sets SMITH.PROJ.ONE and SMITH.PROJ.TWO are protected by generic profile SMITH.PROJ.*, and you want to remove protection from SMITH.PROJ.ONE, create a new profile SMITH.PROJ.ONE with a UACC of ALTER. For specific instructions on creating a discrete profile, see “Creating a discrete profile to protect a data set” on page 57.

Chapter 7. Protecting data on tapes

RACF can protect your data on tapes. It can control who has what authority to access the data. You can use RACF to protect your data on tapes by creating profiles to protect your tape data sets. Talk to your security administrator to find out how tapes are protected at your installation. For more information about tapes, see *z/OS DFSMS Using Magnetic Tapes*.

Chapter 8. Changing access to a data set

Situations might occur when you want to allow or deny someone the use of a data set that you have already protected. You might also want to change how users who are not on a particular data set's access list can use that data set. You can change the access to a data set using the methods described in this chapter.

Changing the universal access authority to a data set

You can allow other users to access a data set by specifying a universal access authority. This access level pertains to any user on the system. For example, if you add confidential research data to a data set, you might want to ensure that the universal access authority of the data set is NONE.

Note: As an alternative to specifying a universal access authority, you can add an entry for ID(*) to the access list to specify an access level that pertains to any RACF-defined user on the system. For more information, see "Using ID(*) in an access list" on page 75.

To change a data set's UACC (universal access authority), you must enter the ALTDSD command with the appropriate operands. To change a data set's UACC:

1. Find the name of the profile that protects the data set. To do this, see "Finding out what data set profiles you have" on page 69.

Remember that changing the UACC for a generic profile changes the access to all data sets protected by the profile.

2. Decide which level of UACC to specify in the profile.

The UACC can be one of the following: NONE, READ, UPDATE, CONTROL, ALTER, or EXECUTE. For descriptions of these values, see "Access authority for data sets" on page 85.

Attention

- a. Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected data set can create a copy of it. As owner of the copied data set, that user has control of the security characteristics of the copied data set, and can downgrade it. For this reason, you might want to initially assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See "Permitting an individual or a group to use a data set" on page 74 for information on how to permit selected users or groups to access a data set.)
- b. If you are changing the UACC to restrict access, be certain that any user or group specifically mentioned in the access list has the access to the resource that you intend. For example, if you change the UACC to NONE, and there is a user specifically named in the access list with any authority, that user still has that authority to the resource.

3. Change the UACC specified in the profile.

To change the UACC, enter the ALTDSD command as follows:

```
ALTDSD 'profile-name' UACC(access-authority)
```

Example 1:

Changing data set access

Assume that data set 'SMITH.PROJ.ONE' is protected by a discrete profile. To change the UACC for this data set to NONE, enter the following command:

```
ALTDSD 'SMITH.PROJ.ONE' UACC(NONE)
```

Example 2:

If you are changing the UACC specified in a generic profile, specify the name of the generic profile. For example, to change the UACC for generic profile SMITH.* to NONE, enter the following command:

```
ALTDSD 'SMITH.*' UACC(NONE)
```

Permitting an individual or a group to use a data set

You can use a data set profile to protect the information you create and use to do your job. Besides protecting a data set with a universal access authority, you can give certain users different abilities to access it, by adding the users and the authority you want to give them to the access list in the data set profile.

Note: For a description of when a change to a user's access occurs, see "When data set profile changes take effect" on page 89.

To permit an individual or a group use of a data set:

1. Find the name of the profile that protects the data set. To do this, see "Finding out how a data set is protected" on page 64.
2. Decide whether to use the profile that protects the data set.
 - If the profile is a discrete profile, go on to Step 3.
 - If the profile is a generic profile, it might protect more than one data set. You need to decide whether to create a new profile for the data set. For more information, see "Choosing between discrete and generic profiles" on page 55.
3. Decide which access authority to specify for the user.

The access authority can be one of the following: NONE, READ, UPDATE, CONTROL, ALTER, or EXECUTE. For descriptions of these values, see "Access authority for data sets" on page 85.

4. Allow access to the data set.

To allow access to your data set, use the PERMIT command with the ACCESS keyword:

```
PERMIT 'profile-name' ID(userID|groupname) ACCESS(level)
```

Example 1. Permitting a user to read a data set

Data set SMITH.PROJ.ONE is protected by a discrete profile. To permit user JONES to read data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(JONES) ACCESS(READ)
```

Example 2. Permitting more than one user to read a data set

To permit users JONES and MOORE to read data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(JONES, MOORE) ACCESS(READ)
```

Example 3. Permitting more than one user or group to read a data set

To permit group DEPTD60 and user JONES to read user data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(DEPTD60, JONES) ACCESS(READ)
```

Example 4. Permitting a user to read a group data set

To permit user SMITH to read group data set GROUPID.PROJ.ONE, enter the following command:

```
PERMIT 'GROUPID.PROJ.ONE' ID(SMITH) ACCESS(READ)
```

Using ID(*) in an access list

You can add an entry for ID(*) to an access list to specify an access level that applies to all RACF-defined users. You can use an entry for ID(*) instead of a UACC, which applies to all users whether or not they are RACF-defined.

Note: Neither an ID(*) entry nor a UACC applies to users who have the RESTRICTED attribute.

The following examples illustrate the difference between using a UACC and using an entry for ID(*) to give read access to a data set. Assume that data set SMITH.PROJ.ONE is protected by a discrete profile.

- To allow all users on the system to read the data set, specify UACC(READ) for the profile, as follows:

```
ALTDSD 'SMITH.PROJ.ONE' UACC(READ)
```

- To allow only RACF-defined users on the system to read the data set, specify UACC(NONE) for the profile, then issue the PERMIT command with ID(*) and ACCESS(READ) specified:

```
ALTDSD 'SMITH.PROJ.ONE' UACC(NONE)
PERMIT 'SMITH.PROJ.ONE' ID(*) ACCESS(READ)
```

Denying an individual or a group use of a data set

You can use a data set profile to protect the information in your data sets. You might want to deny an individual use of a data set. For example, a colleague who has left the department can still use a data set. For security reasons you wish to exclude the person from using the data set. You can deny anyone access to your data set by specifying a certain universal access or individual access authority.

Note: For a description of when a change to a user's access occurs, see "When data set profile changes take effect" on page 89.

To deny an individual or a group use of a data set:

1. Find the name of the profile that protects the data set. To do this, see "Finding out how a data set is protected" on page 64.
2. Decide whether to use the profile that protects the data set.
 - If the profile is a discrete profile, go on to Step 3.
 - If the profile is a generic profile, it might protect more than one data set. You need to decide whether to create a new profile for the data set. For more information, see "Choosing between discrete and generic profiles" on page 55.
3. Use the PERMIT command to deny access to the data set.

You can use the PERMIT command to do this in two ways:

- One way to deny access is to include the user or group on the access list but assign the user or group an access of NONE. To assign an access of NONE is the best procedure to ensure that the user or group has no access to the data set. See "Including the individual or group on the access list with ACCESS(NONE)" on page 76.
- The second way is to remove the name of the user or group from the access list. However, this denies access only if the UACC is NONE. For example, if

Changing data set access

you delete a user or group from the access list but the UACC is READ or higher, the user or group can still access the data set. See “Removing the user or group from the access list.”

Including the individual or group on the access list with ACCESS(NONE)

Including the user or group on the access list with ACCESS(NONE) ensures that the user or group is denied access the data set.

To deny access by assigning a user or group an access of NONE, enter the PERMIT command with the ACCESS keyword as follows:

```
PERMIT 'profile-name' ID(userid|groupname) ACCESS(NONE)
```

Example 1:

To deny user JONES the use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(JONES) ACCESS(NONE)
```

Example 2:

To deny users JONES and MOORE the use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(JONES, MOORE) ACCESS(NONE)
```

Example 3:

To deny group DEPTD60 the use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(DEPTD60) ACCESS(NONE)
```

Example 4:

To deny groups DEPTD60 and DEPTD58 use of user data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(DEPTD60, DEPTD58) ACCESS(NONE)
```

Removing the user or group from the access list

To deny access by removing a user or a group from the access list, enter the PERMIT command with DELETE keyword as follows:

```
PERMIT 'profile-name' ID(userid|groupname) DELETE
```

Example 1:

To deny user JONES use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(JONES) DELETE
```

Example 2:

To deny users JONES and MOORE use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(JONES, MOORE) DELETE
```

Example 3:

To deny group DEPTD60 the use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(DEPTD60) DELETE
```

Example 4:

To deny groups DEPTD60 and DEPTD58 the use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(DEPTD60, DEPTD58) DELETE
```

Changing data set access

Chapter 9. Protecting general resources

The types of general resources that RACF can protect include:

- DASD volumes
- Tape volumes
- Load modules (programs)
- Application resources (such as resources for IMS™, CICS, and DB2®)
- Terminals
- Installation-defined resources

For a complete list, see “Supplied RACF resource classes” on page 91.

Resources are protected with profiles. A profile contains descriptive information about a user, a group, or resource. RACF uses the information in a profile to control use of protected resources. When you attempt to use a protected resource, RACF checks your user profile, as well as the resource profile, to decide whether to allow you to use the resource.

Resource profiles describe the information and the levels of authority needed to use the resource. A resource profile contains:

- The resource name and resource owner.
- The access list, which is a list of users who can use a resource and how they can use it.
- The universal access authority (UACC), which is the default level of access authority allowed for all users who are not listed in the access list.
- Auditing information. RACF can audit the use of each resource. The audit can be general or specific. For example, you can set up a resource profile for your resource to audit every attempt to use that resource. Or, you can define the profile to audit only the attempts to update the resource.

You can protect a resource by identifying specific users with the access you want them to have in the access list. All other users are allowed the access you specify as the universal access authority (UACC). The access authorities you can specify are: NONE, READ, UPDATE, CONTROL, and ALTER. See “Access authority for general resources” on page 86 for more information about access authorities. To protect a resource most effectively, you should initially specify a UACC of NONE and selectively give certain users specific access authority to the resource.

Note: The security administrator is *generally* the person who defines, alters, or deletes a general resource profile.

You can use RACF to protect your general resources by doing the tasks defined in this chapter.

Searching for general resource profile names

You can list the names of general resource profiles that you own by using the SEARCH command.

The SEARCH command searches the RACF database for the names of profiles (in a particular resource class) that match the criteria you specify. For example, you

Protecting general resources

can search for all TERMINAL profiles. Profiles that are listed are those you are the owner of, or to which you have at least READ access authority.

The output of this command is in line mode unless you use ISPF panels. You can use the TSO session manager to scroll through the output from the listing commands. By using the CLIST operand, you can save the list of profile names in a data set.

Attention: Using the SEARCH command can slow the system's performance. Therefore, the SEARCH command should be used with discretion (or not at all) during busy system times.

1. Find the name of the class that represents the resource you want to search. Valid class names are DATASET, USER, GROUP, and those names specified in the class descriptor table (CDT). For a list of the general resource classes that are defined in the class descriptor table supplied by IBM, see "Supplied RACF resource classes" on page 91.
2. Request the list of RACF profiles for the class. To search the RACF database for general resource profiles that you own, use the SEARCH command with the CLASS operand. Enter `search class(classname)` to find all the general resources you can access, this must be done one class at a time.

Example:

To search for resource profiles in class TERMINAL, type: `SEARCH CLASS(TERMINAL)`

These examples show only some of the operands that are available to use on the SEARCH command. The complete syntax of the SEARCH command, with descriptions of all the command operands, is described in *z/OS Security Server RACF Command Language Reference*. In particular, you might want to read about these operands:

- CLIST
Specifies RACF commands (or other commands) to be saved with the profile names, generating a CLIST that you run against the profiles.
- FILTER
Specifies a string of characters to be used in searching the RACF database. The filter string defines the range of profile names you want to select from the RACF database.

Listing the contents of general resource profiles

You can list the contents of general resource profiles that you own by using the RLIST command.

The RLIST command lists the contents of general resource profiles in a particular resource class. If you specify a profile that you do not have access to, you might receive an "access violation" message from the RLIST command.

Note: To see the access list for a resource, you must be the owner of the resource, or have ALTER access to the resource.

1. Find the name of the class that represents the resource you want to search. Valid class names are those specified in the class descriptor table (CDT). For a list of general resource classes defined in the class descriptor table supplied by IBM, see "Supplied RACF resource classes" on page 91.

- Specify the RACF profiles you want to list. To list the contents of general resource profiles that you own, use the RLIST command with the class name and a profile name. Type:

```
RLIST classname profile-name
```

Example 1:

To list the contents of resource profile IDTERMS in class TERMINAL, type:

```
RLIST TERMINAL IDTERMS
```

Example 2:

To list the contents of all resource profiles in class TERMINAL, type:

```
RLIST TERMINAL *
```

These examples show only some of the operands that are available to use on the RLIST command. The complete syntax of the RLIST command, with descriptions of all the command operands, is described in *z/OS Security Server RACF Command Language Reference*. In particular, you might want to read about these operands:

- ALL
Displays all information specified for each resource.
- AUTHUSER
Displays the standard and conditional access lists for the profile. This is useful information to have before you use the PERMIT command to allow or deny access to the resource.

Permitting an individual or a group to use a general resource

You can give certain users or groups of users different access authorities to use a general resource. You add their user IDs and the authority you want to give them to the access list on the resource profile. For example, if you would like J.E. Jones, whose user ID is JONES, to use your RACF-protected terminal, you would add his user ID to its access list.

To permit an individual or a group to use a general resource:

- Find the name of the profile that protects the general resource. To do this, see “Searching for general resource profile names” on page 79.
- Decide which access authority to specify in the profile. The access authority can be one of the following: NONE, READ, UPDATE, CONTROL, and ALTER. For descriptions of these values, see “Access authority for general resources” on page 86.
- Allow access to the general resource. To allow access to your general resource, use the PERMIT command with the ACCESS operand. Type:

```
PERMIT profile-name CLASS(classname) ID(userid|groupname)  
ACCESS(access-authority)
```

You can specify * on the ID operand to allow all non-RESTRICTED RACF-defined users to have the access that you specify on the ACCESS operand.

Example 1:

To permit user Jones to have access to a terminal protected by general resource profile IDTERMS, type:

Protecting general resources

```
PERMIT IDTERMS CLASS(TERMINAL) ID(JONES) ACCESS(READ)
```

Example 2:

To permit groups DEPTD60 and DEPTD58 to have access to a terminal protected by general resource profile IDTERMS, type:

```
PERMIT IDTERMS CLASS(TERMINAL) ID(DEPTD60, DEPTD58) ACCESS(READ)
```

Example 3:

To permit all RACF-defined users to have access to a terminal protected by general resource profile IDTERMS, type:

```
PERMIT IDTERMS CLASS(TERMINAL) ID(*) ACCESS(READ)
```

These examples show only some of the operands that are available to use on the PERMIT command. The complete syntax of the PERMIT command, with descriptions of all the command operands, is described in *z/OS Security Server RACF Command Language Reference*.

Denying an individual or a group use of a general resource

You might want to deny an individual or group use of a general resource. For example, a colleague who has left the department can still use a general resource. For security reasons you would wish to exclude the person from using the general resource. You can deny a person access to your general resource by specifying a certain universal access or individual access authority.

To deny an individual or a group the use of a general resource:

1. Find the name of the profile that protects the general resource. To do this, see “Searching for general resource profile names” on page 79.
2. Deny access to the general resource. You can deny access in one of two ways:
 - One way is to remove the name of the user or group from the access list. However, this denies access only if the UACC is NONE. For example, if you delete a user or group from the access list but the UACC is READ or higher, the user or group still has access to the general resource. See “Removing the individual or group from the access list” on page 83.
 - The second way to deny access is to include the user or group on the access list but assign the user or group an access of NONE. By assigning an access of NONE, you make sure the user or group cannot access the general resource. See “Including the individual or group on the access list with ACCESS(NONE).”

Including the individual or group on the access list with ACCESS(NONE)

By including the user or group on the access list with ACCESS(NONE), you make sure that the user or group cannot access the general resource. To deny access by assigning a user or group an access of NONE, enter the PERMIT command with the ACCESS keyword as follows:

```
PERMIT profile-name CLASS(classname) ID(userid|groupname) ACCESS(NONE)
```

Example 1:

To deny user Jones use of a terminal protected by general resource profile IDTERMS, type:

```
PERMIT IDTERMS CLASS(TERMINAL) ID(JONES) ACCESS(NONE)
```

Example 2:

To deny groups DEPTD60 and DEPTD58 use of a terminal protected by general resource profile IDTERMS, type:

```
PERMIT IDTERMS CLASS(TERMINAL) ID(DEPTD60, DEPTD58) ACCESS(NONE)
```

These examples show only some of the operands that are available to use on the PERMIT command. The complete syntax of the PERMIT command, with descriptions of all the command operands, is described in *z/OS Security Server RACF Command Language Reference*. In particular, you might want to read about this operand:

- RESET

Deletes the entire contents of both the standard access list and the conditional access list of a profile.

Removing the individual or group from the access list

To revert to the universal access authority for a user or a group, enter the PERMIT command with the DELETE operand. Type:

```
PERMIT profile-name CLASS(classname) ID(userid|groupname) DELETE
```

Example 1:

To remove user Jones from the access list for a terminal protected by general resource profile IDTERMS, type:

```
PERMIT IDTERMS CLASS(TERMINAL) ID(JONES) DELETE
```

Access to the terminal for user Jones reverts to the universal access authority for the terminal.

Example 2:

To remove groups DEPTD60 and DEPTD58 from the access list for a terminal protected by general resource profile IDTERMS, type:

```
PERMIT IDTERMS CLASS(TERMINAL) ID(DEPTD60, DEPTD58) DELETE
```

Access to the terminal for groups DEPTD60 and DEPTD58 reverts to the universal access authority for the terminal.

These examples show only some of the operands that are available to use on the PERMIT command. The complete syntax of the PERMIT command, with descriptions of all the command operands, is described in *z/OS Security Server RACF Command Language Reference*. In particular, you might want to read about this operand:

- RESET

Deletes the entire contents of both the standard access list and the conditional access list of a profile.

Appendix A. Reference summary

The following sections contain reference information about RACF.

Access authority for data sets

These definitions apply both to UACC authority and to authority granted to individual users or groups in the data set profile access list. Access authority for data sets can be:

NONE Does not allow users to access the data set.

Attention

Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected data set can create a copy of it. As owner of the copied data set, that user has control of the security characteristics of the copied data set, and can downgrade it. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See “Permitting an individual or a group to use a data set” on page 74 for information on how to permit selected users or groups to access a data set.)

READ Allows users to access the data set for reading only. (Note that users who can read the data set can copy or print it.)

UPDATE

Allows users to read from, copy from, or write to the data set. UPDATE does not, however, authorize a user to delete, rename, move, or scratch the data set.

Allows users to perform normal VSAM I/O (not improved control interval processing) to VSAM data sets.

CONTROL

For VSAM data sets, CONTROL is equivalent to the VSAM CONTROL password; that is, it allows users to perform improved control interval processing. This is control-interval access (access to individual VSAM data blocks), and the ability to retrieve, update, insert, or delete records in the specified data set.

For non-VSAM data sets, CONTROL is equivalent to UPDATE.

ALTER

ALTER allows users to read, update, delete, rename, move, or scratch the data set.

When specified in a discrete profile, ALTER allows users to read, alter, and delete the profile itself *including the access list*.

Note: ALTER does not allow users to change the owner of the profile using the ALTDS command. However, if a user with ALTER access authority to a discrete data set profile renames the data set, changing the high-level qualifier to his or her own user ID, then both the data set and the profile are renamed, *and* the OWNER of the profile is changed to the new user ID.

Reference information

When specified in a generic profile, ALTER gives users *no* authority over the profile itself, but lets users create new data sets that are covered by that profile.

EXECUTE

For a private load library, EXECUTE lets users load and execute, but not read or copy, programs (load modules) in the library.

Note: In order to specify EXECUTE for a private load library, you must ask for assistance from your RACF security administrator.

Access authority for general resources

These definitions apply both to UACC authority and to authority granted to individual users or groups in the resource profile access list.

The UACC is the default **resource-access authority**. All users or groups of users in the system who are not specifically named in an access list of authorized users for that resource can still access the resource with the authority specified by the UACC. The UACC also applies to users not defined to RACF.

Note: These access authorities can have different meanings depending on the general resource they are protecting. *z/OS Security Server RACF Security Administrator's Guide* describes the meaning of the access authorities for each kind of general resource. Additional information should be found in the reference materials for the specific product.

The resource access authorities are:

ALTER

Specifies that the user or group have full control over the resource.

CONTROL

Is used only for VSAM data sets and specifies that the user or group have access authority that is equivalent to the VSAM control password.

UPDATE

Specifies that the user or group be authorized to access the resource for the purpose of reading or writing.

READ Specifies that the user or group be authorized to access the resource for the purpose of reading only.

EXECUTE

Specifies that the user or group can run programs but not read or copy them.

NONE Specifies that the user or group not be permitted to access the resource.

Profile names for data sets

The enhanced generic naming (EGN) option changes the meaning of generic characters within profile names. To find out if EGN is active at your installation, ask your security administrator.

Generic profile rules when enhanced generic naming is inactive

In the DATASET class, you can use generic characters as follows:

- Specify % to match any single character in a data set name

- Specify * as follows:
 - As a character at the end of a data set profile name (for example, ABC.DEF*) to match zero or more characters until the end of the name, zero or more qualifiers until the end of the data set name, or both
 - As a qualifier at the end of a profile name (for example, ABC.DEF.*) to match one or more qualifiers until the end of the data set name
 - As a qualifier in the middle of a profile name (for example, ABC.*.DEF) to match any one qualifier in a data set name
 - As a character at the end of a qualifier in the middle of a profile name (for example, ABC.DE*.FGH) to match zero or more characters until the end of the qualifier in a data set name.

Note: For profiles in the DATASET class, the high-level qualifier of the profile name must not be, nor can it contain, a generic character—for example, *.ABC, AB%.B, and AB*.AB are not allowed.

The following tables are provided to show the variety of profiles that can be created by using generics, and by using enhanced generic naming. They also show the effects on profile protection if enhanced generic naming is turned off.

Table 2 and Table 3 provide examples of data set names using generic naming. Enhanced generic naming has not been turned on (SETROPTS NOEGN, the default, is in effect).

Table 4 and Table 5 provide examples of data set names with enhanced generic naming (SETR EGN is on).

*Table 2. Generic naming for data sets with enhanced generic naming inactive: * at the end*

Profile Name	AB.CD*	AB.CD.*
Resources protected by the profile	AB.CD AB.CDEF AB.CD.EF AB.CD.XY AB.CD.EF.GH	AB.CD.EF AB.CD.XY AB.CD.EF.GH
Resources not protected by the profile	ABC.DEF ABC.XY.XY.DEF	AB.CD AB.CDEF ABC.DEF AB.XY.XY.DEF

*Table 3. Generic naming for data sets with enhanced generic naming inactive: * in the middle or %*

Profile Name	ABC.%EF	AB.*.CD	AB.CD*.EF
Resources protected by the profile	ABC.DEF ABC.XEF	AB.CD.CD	AB.CDEF.EF AB.CDE.EF
Resources not protected by the profile	ABC.DEFGHI ABC.DEF.GHI ABC.DDEF	AB.CD AB.CD.EF AB.CDEF ABC.DEF ABC.XY.CD AB.XY.XY.CD	AB.CD.XY.EF

Reference information

Generic profile rules when enhanced generic naming is active

The *enhanced generic naming* option applies only to data sets and allows you to use double asterisks (**) in the DATASET class. It also changes the meaning of the single asterisk (*) at the end of a profile name.

Your RACF security administrator activates enhanced generic naming by issuing the SETROPTS command with the EGN operand. SETROPTS EGN makes the rules for data set and general resource profiles consistent with each other. Additionally, generic profiles can be more precise, and the generic profile names are more similar to other IBM products.

New installations should set EGN on immediately.

The following rules apply if you have enhanced generic naming in effect.

Specify * as follows:

- As a character at the end of a data set profile name to match zero or more characters until the end of the qualifier.
- As a qualifier at the end of a profile name to match *one* qualifier until the end of the data set name.

Note: There are differences in the meaning of an ending asterisk, depending on whether an installation is using generic profiles with or without EGN.

Specify ** as follows:

- As either a middle or end qualifier in a profile name to match zero or more qualifiers. Only one occurrence of a double asterisk is allowed in a profile name. For example, ABC.DE.** is allowed; ABC.DE** is not allowed; and A.**.B.** is not allowed.

Note: RACF does not allow you to specify any generic characters in the high-level qualifier of a data set name.

Table 4 and Table 5 on page 89 show examples of generic profile names you can create when enhanced generic naming is active, and the resources protected and not protected by those profiles.

Table 4. Generic data set profile names created with enhanced generic naming active: * and **

Profile name	A.B*	A.B.*	A.B.**	A.B*.**	A.B.*.**
Resources protected by the profile	A.B A.BC	A.B.C A.B.X	A.B A.B.C A.B.C.D A.B.X	A.B A.B.C A.BC A.BC.D A.B.C.D A.B.X	A.B.C A.B.C.D A.B.X
Resources not protected by the profile	A.B.C A.B.C.D A.B.X AB.CD	A.B A.BC A.B.C.D AB.CD	A.BC A.BC.D AB.CD	AB.CD	AB.CD A.BC A.BC.D A.B AB.X.Y.C

Table 5. Generic data set profile names created with enhanced generic naming active: *, **, or % in the middle

Profile name	ABC.%EF	AB.*.CD	AB.**.CD
Resources protected by the profile	ABC.DEF ABC.XEF	AB.CD.CD	AB.CD AB.X.CD AB.X.Y.CD
Resources not protected by the profile	ABC.DEFGHI ABC.DEF.GHI ABC.DDEF	AB.CD AB.CD.EF AB.CDEF ABC.DEF ABC.XY.CD ABC.XY.XY.CD	AB.CD.EF AB.CDEF ABC.X.CD.EF ABC.DEF ABX.YCD

Note: Although multiple generic profiles might match a data set name, only the most specific actually protects the data set. For example, AB.CD*, AB.CD.**, and AB.**.CD all match the data set AB.CD, but AB.CD* protects the data set.

In general, given two profiles that match a data set, you can find the more specific one by comparing the profile name from left to right. Where they differ, a non-generic character is more specific than a generic character. In comparing generics, a % is more specific than an *, and an * is more specific than **. Another way to determine the most specific is with the SEARCH command, as there are some rare exceptions to the general rule. SEARCH always lists the profiles in the order of the most specific to the least specific.

When data set profile changes take effect

If a user is currently using a data set, changing the data set profile protecting the data set might not affect the user's current access until that user logs on again.

The change affects the user's access immediately in the following cases:

- If the user is not logged on. You can check to see if a user is logged on with the TSO STATUS command:

```
STATUS userid
```

If the user is logged on, the system displays a message indicating that a job with the letters TSU in it is executing.

- If the user is logged on and has not yet opened the data set or a data set protected by the same generic profile (for example, by browsing or editing).

If the user is logged on and has opened the data set, and you change his access, two situations could occur:

- If the profile is a discrete profile, the user's access changes after closing the data set.
- If the profile is a generic profile, the user's access changes after *one* of the following occurs:
 - The user issues the LISTDSD command as follows:


```
LISTDSD DATASET(data-set-protected-by-the-profile) GENERIC
```

 This places a fresh copy of the profile in the user's address space.
 - A SETROPTS GENERIC(DATASET) REFRESH is issued on the system the user is logged on to.

Reference information

Note: This command cannot be issued by a general user. It can be issued only by someone with the SPECIAL, OPERATIONS, or AUDITOR attribute.

- The user references more than four data sets with different high-level qualifiers, and the data sets are protected by generic profiles.
- The user logs off and then logs back on.

Automatic direction of application updates

While running, an application can make updates to the RACF database. For example, if a user enters an incorrect logon password, an application updates the RACF database to increment the count of incorrect passwords. Updates are also made when a user creates, deletes, or renames a data set that is protected by a discrete profile. In this case, updates are made to maintain the data set profile.

Automatic direction of application updates, a function of the RACF remote sharing facility, is primarily used to keep already-synchronized RACF profiles synchronized between two or more remote nodes. Automatic direction of application updates propagates each individual update. Propagation of an application update takes place only after the update has successfully completed on the node where the application is running and only if SET AUTOAPPL has been used to activate automatic direction on that node.

An installation decides who should be notified of results and output from automatically directed application updates, so a user might or might not see output or TSO SEND messages from automatically directed application updates. If you receive output or notification that an automatically directed application update failed, notify your RACF security administrator.

Figure 49 shows the sample output of a successful application update. In this example, RACF sets the revoke count for a non-valid password attempt.

```
=====
Application update request issued at 15:49:27 on 03/17/98 was
processed at NODE4.RRSFU1 on 03/17/98 at 15:49:28
Request was propagated by automatic direction from NODE3.RRSFU1

REQUEST ISSUED: ICHEINTY ALTER operation from user NODE3.RRSFU1

REQUEST OUTPUT:
IRRR101I Application update request completed successfully
           for class USER, profile name RRSFU1.
=====
```

Figure 49. A successful application update: sample output

Figure 50 on page 91 shows the sample output when RACF attempts to set the revoke count for a non-valid password attempt, but fails because the user ID is already revoked.

```

=====
Application update request issued at 15:49:27 on 03/17/98 was *not*
processed at NODE4.RRSFU1 on 03/17/98 at 15:49:28
Request was propagated by automatic direction from NODE3.RRSFU1

REQUEST ISSUED: ICHEINTY ALTER operation from user NODE3.RRSFU1

ERROR INFORMATION:
IRRC110I Unable to establish RACF environment for application update request
IRRC021I ACCESS HAS BEEN REVOKED FOR USER ID RRSFU1.
=====

```

Figure 50. When the user ID is revoked: sample output

Supplied RACF resource classes

This appendix describes the general resource classes you can find in the supplied class descriptor table (CDT) and contains the following sections:

- “Supplied resource classes for z/OS systems”
- “Supplied resource classes for z/VM systems” on page 99

See *z/OS Security Server RACF Macros and Interfaces* to find the details (such as POSIT values) associated with the CDT entry for each class.

Supplied resource classes for z/OS systems

Table 6 lists the supplied CDT classes that can be used on z/OS systems. See restrictions at the end of the table.

Table 6. Resource classes for z/OS systems

Class name	Description
ALCSAUTH	Supports the Airline Control System/MVS (ALCS/MVS) product.
APPCLU	Verifying the identity of partner logical units during VTAM® session establishment.
APPCPORT	Controlling which user IDs can access the system from a given LU (APPC port of entry). Also, conditional access to resources for users entering the system from a given LU.
APPCSERV	Controlling whether a program being run by a user can act as a server for a specific APPC transaction program (TP).
APPCSI	Controlling access to APPC side information files.
APPCTP	Controlling the use of APPC transaction programs.
APPL	Controlling access to applications.
CACHECLS	Contains profiles used for saving and restoring cache contents from the RACF database.
CBIND	Controlling the client's ability to bind to the server.
CDT	Contains profiles for installation-defined classes for the dynamic CDT. ³
CFIELD	Contains profiles that define the installation's custom fields. ³
CONSOLE	Controlling access to MCS consoles. Also, conditional access to other resources for commands originating from an MCS console.
DASDVOL	DASD volumes.
DBNFORM	Reserved for future IBM use.

Table 6. Resource classes for z/OS systems (continued)

Class name	Description
DEVICES	Used by MVS allocation to control who can allocate devices such as: <ul style="list-style-type: none"> • Unit record devices (printers and punches) (allocated only by PSF, JES2, or JES3) • Graphics devices (allocated only by VTAM) • Teleprocessing (TP) or communications devices (allocated only by VTAM)
DIGTCERT	Contains digital certificates and information related to them.
DIGTCRIT	Specifies additional criteria for certificate name filters.
DIGTNMAP	Mapping class for certificate name filters.
DIGTRING	Contains a profile for each key ring and provides information about the digital certificates that are part of each key ring.
DIRAUTH	Setting logging options for RACROUTE REQUEST=DIRAUTH requests. Also, if the DIRAUTH class is active, security label authorization checking is done when a user receives a message sent through the TPUT macro or the TSO SEND, or LISTBC commands. ⁵
DLFCLASS	The data lookaside facility.
FACILITY	Miscellaneous uses. Profiles are defined in this class so resource managers (typically elements of z/OS or z/VM) can check a user's access to the profiles when the user takes some action. Examples are the profiles used to control execution of RACDCERT command functions and the profiles used to control privileges in the z/OS UNIX environment. RACF does not document all of the resources used in the FACILITY class by other products. For information on the FACILITY class resources used by a specific product (other than RACF itself), see that product's documentation.
FIELD	Fields in RACF profiles (field-level access checking).
GDASDVOL	Resource group class for DASDVOL class. ¹
GLOBAL	Global access checking table entry. ¹
GMBR	Member class for the GLOBAL class. ⁴
GSDSF	Resource group class for SDSF class. ¹
GTERMINL	Resource group class for TERMINAL class. ¹
GXFACILI	Grouping class for XFACILIT resources.
IBMOPC	Controlling access to OPC/ESA subsystems.
IDIDMAP	Contains distributed identity filters created with the RACMAP command.
JESINPUT	Conditional access support for commands or jobs entered into the system through a JES input device.
JESJOBS	Controlling the submission and cancellation of jobs by job name.
JESSPOOL	Controlling access to job data sets on the JES spool (that is, SYSIN and SYSOUT data sets).
KEYSMSTR	Contains profiles that hold keys to encrypt data stored in the RACF database, such as LDAP BIND passwords and DCE passwords.
LDAPBIND	Contains the LDAP server URL, bind distinguished name, and bind password.
LOGSTRM	Controls system logger resources, such as log streams and the coupling facility structures associated with log streams.

Table 6. Resource classes for z/OS systems (continued)

Class name	Description
NODES	Controlling the following on MVS systems: <ul style="list-style-type: none"> • Whether jobs are allowed to enter the system from other nodes • Whether jobs that enter the system from other nodes have to pass user identification and password verification checks
NODMBR	Member class for the NODES class. ⁴
OPERCMD5	Controlling who can issue operator commands (for example, JES and MVS, and operator commands). ²
PMBR	Member class for the PROGRAM class. ⁴
PROGRAM	Protects executable programs. ¹
PROPCNTL	Controlling if user ID propagation can occur, and if so, for which user IDs (such as the CICS or IMS main task user ID), user ID propagation is <i>not</i> to occur.
PSFMPL	Used by PSF to perform security functions for printing, such as separator page labeling, data page labeling, and enforcement of the user printable area.
PTKTDATA	PassTicket key class enables the security administrator to associate a RACF secured signon secret key with a particular mainframe application that uses RACF for user authentication. Examples of such applications are IMS, CICS, TSO, z/VM, APPC, and MVS batch.
RACFEVNT	Contains profiles that control the following events: <ul style="list-style-type: none"> • LDAP change log notification for changes to certain RACF profiles • New password and password phrase enveloping for a given user.
RACFHC	Used by IBM Health Checker for z/OS. Contains profiles that list the resources to check for each installation-defined health check. ¹
RACFVARS	RACF variables. In this class, profile names, which start with & (ampersand), act as RACF variables that can be specified in profile names in other RACF general resource classes.
RACGLIST	Class of profiles that hold the results of RACROUTE REQUEST=LIST,GLOBAL=YES or a SETROPTS RACLIST operation.
RACHCMBR	Used by IBM Health Checker for z/OS. Member class for the RACHCMBR class. ¹
RDATA LIB	Used to control use of the R_data lib callable service (IRRSIDL00 or IRRSDL64).
RRSFDATA	Used to control RACF remote sharing facility (RRSF) functions.
RVARSMBR	Member class for the RACFVARS class. ⁴
SCDMBR	Member class for the SECDATA class. ⁴
SDSF	Controls the use of authorized commands in the System Display and Search Facility (SDSF). See also GSDSF class.
SECDATA	Security classification of users and data (security levels and security categories). ¹
SECLABEL	If security labels are used, and, if so, their definitions. ²
SECLMBR	Member class for the SECLABEL class. ⁴
SERVAUTH	Contains profiles used by servers to check a client's authorization to use the server or to use resources managed by the server. Also, can be used to provide conditional access to resources for users entering the system from a given server.
SERVER	Controlling the server's ability to register with the daemon.

Table 6. Resource classes for z/OS systems (continued)

Class name	Description
SMESSAGE	Controlling to which users a user can send messages (TSO only).
SOMDOBJS	Controlling the client's ability to invoke the method in the class.
STARTED	Used in preference to the started procedures table to assign an identity during the processing of an MVS START command.
SURROGAT	If surrogate submission is allowed, and if allowed, which user IDs can act as surrogates.
SYSMVIEW	Controlling access by the SystemView® for MVS Launch Window to SystemView for MVS applications.
TAPEVOL	Tape volumes.
TEMPDSN	Controlling who can access residual temporary data sets. ⁵
TERMINAL	Terminals (TSO or z/VM). See also GTERMINL class.
VTAMAPPL	Controlling who can open ACBs from non-APF authorized programs.
WRITER	Controlling the use of JES writers.
XFACILIT	Miscellaneous uses. Profile names in this class can be longer than 39 characters in length. Profiles are defined in this class so that resource managers (typically elements of z/OS) can check a user's access to the resources when the users take some action.
CICS classes	
ACICSPCT	CICS program control table. ²
BCICSPCT	Resource group class for the ACICSPCT class. ¹
CCICSCMD	Used to verify that a user is permitted to use CICS system programmer commands such as INQUIRE, SET, PERFORM, and COLLECT. ¹
CPSMOBJ	Used by CICSplex® System Manager, which provides a central point of control when running multiple CICS systems, to determine operational controls within a CICS complex.
CPSMXMP	Used by CICSplex System Manager to identify exemptions from security controls within a CICS complex.
DCICSDCT	CICS destination control table. ²
ECICSDCT	Resource group class for the DCICSDCT class. ¹
FCICSFCT	CICS file control table. ²
GCICSTRN	Resource group class for TCICSTRN class. ²
GCPSMOBJ	Resource grouping class for CPSMOBJ.
HCICSFCT	Resource group class for the FCICSFCT class. ¹
JCICSJCT	CICS journal control table. ²
KCICSJCT	Resource group class for the JCICSJCT class. ¹
MCICSPPT	CICS processing program table. ²
NCICSPPT	Resource group class for the MCICSPPT class. ¹
PCICSPSB	CICS program specification blocks (PSBs).
QCICSPSB	Resource group class for the PCICSPSB class. ¹
RCICSRES	CICS document templates.
SCICSTST	CICS temporary storage table. ²
TCICSTRN	CICS transactions.
UCICSTST	Resource group class for SCICSTST class. ¹

Table 6. Resource classes for z/OS systems (continued)

Class name	Description
VCICSCMD	Resource group class for the CCICSCMD class. ¹
WCICSRES	Resource group class for the RCICSRES class.
DB2 classes	
DSNADM	DB2 administrative authority class.
DSNR	Controls access to DB2 subsystems.
GDSNBP	Grouping class for DB2 buffer pool privileges.
GDSNCL	Grouping class for DB2 collection privileges.
GDSNDB	Grouping class for DB2 database privileges.
GDSNJR	Grouping class for Java™ archive files (JARs).
GDSNPK	Grouping class for DB2 package privileges.
GDSNPN	Grouping class for DB2 plan privileges.
GDSNSC	Grouping class for DB2 schemas privileges.
GDSNSG	Grouping class for DB2 storage group privileges.
GDSNSM	Grouping class for DB2 system privileges.
GDSNSP	Grouping class for DB2 stored procedure privileges.
GDSNSQ	Grouping class for DB2 sequences.
GDSNTB	Grouping class for DB2 table, index, or view privileges.
GDSNTS	Grouping class for DB2 tablespace privileges.
GDSNUF	Grouping class for DB2 user-defined function privileges.
GDSNUT	Grouping class for DB2 user-defined distinct type privileges.
MDSNBP	Member class for DB2 buffer pool privileges.
MDSNCL	Member class for DB2 collection privileges.
MDSNDB	Member class for DB2 database privileges.
MDSNJR	Member class for Java archive files (JARs).
MDSNPK	Member class for DB2 package privileges.
MDSNPN	Member class for DB2 plan privileges.
MDSNSC	Member class for DB2 schema privileges.
MDSNSG	Member class for DB2 storage group privileges.
MDSNSM	Member class for DB2 system privileges.
MDSNSP	Member class for DB2 stored procedure privileges.
MDSNSQ	Member class for DB2 sequences.
MDSNTB	Member class for DB2 table, index, or view privileges.
MDSNTS	Member class for DB2 tablespace privileges.
MDSNUF	Member class for DB2 user-defined function privileges.
MDSNUT	Member class for DB2 user-defined distinct type privileges.
DCE class	
DCEUIDS	Used to define the mapping between a user's RACF user ID and the corresponding DCE principal UUID.
Enterprise Identity Mapping (EIM) class	
RAUDITX	Controls auditing for Enterprise Identity Mapping (EIM).

Table 6. Resource classes for z/OS systems (continued)

Class name	Description
Enterprise Java Beans classes	
EJBROLE	Member class for Enterprise Java Beans authorization roles.
GEJBROLE	Grouping class for Enterprise Java Beans authorization roles.
JAVA	Contains profiles that are used by Java for z/OS applications to perform authorization checking for Java for z/OS resources.
IMS classes	
AIMS	Application group names (AGN).
CIMS	Command.
DIMS	Grouping class for command.
FIMS	Field (in data segment).
GIMS	Grouping class for transaction.
HIMS	Grouping class for field.
IIMS	Program specification block (PSB).
JIMS	Grouping class for program specification block (PSB).
LIMS	Logical terminal (LTERM).
MIMS	Grouping class for logical terminal (LTERM).
OIMS	Other.
PIMS	Database.
QIMS	Grouping class for database.
RIMS	Open Transaction Manager Access (OTMA) transaction pipe (TPIPE).
SIMS	Segment (in database).
TIMS	Transaction (trancode).
UIMS	Grouping class for segment.
WIMS	Grouping class for other.
Integrated Cryptographic Service Facility (ICSF) classes	
CRYPTOZ	Controls access to PKCS #11 tokens.
CSFKEYS	Controls access to ICSF cryptographic keys.
CSFSERV	Controls access to ICSF cryptographic services.
GCSFKEYS	Resource group class for the CSFKEYS class. ¹
GXCSFKEY	Resource group class for the XCSFKEY class. ¹
XCSFKEY	Controls the exportation of ICSF cryptographic keys.
Infoprint Server class	
PRINTSRV	Controls access to printer definitions for Infoprint Server.
Information/Management (Tivoli® Service Desk) classes	
GINFOMAN	Grouping class for Information/Management (Tivoli Service Desk) resources.
INFOMAN	Member class for Information/Management (Tivoli Service Desk) resources.
LFS/ESA classes	
LFSCCLASS	Controls access to file services provided by LFS/ESA.
License Manager class	

Table 6. Resource classes for z/OS systems (continued)

Class name	Description
ILMADMIN	Controls access to the administrative functions of IBM License Manager.
Lotus Notes for z/OS and Novell Directory Services for OS/390 classes	
NDSLINK	Mapping class for Novell Directory Services for OS/390 user identities.
NOTELINK	Mapping class for Lotus Notes for z/OS user identities.
MQSeries® classes	
GMQADMIN	Grouping class for MQSeries administrative options. ¹
GMQCHAN	Reserved for MQSeries.
GMQNLIST	Grouping class for MQSeries namelists. ¹
GMQPROC	Grouping class for MQSeries processes. ¹
GMQQUEUE	Grouping class for MQSeries queues. ¹
MQADMIN	Protects MQSeries administrative options.
MQCHAN	Reserved for MQSeries.
MQCMDS	Protects MQSeries commands.
MQCONN	Protects MQSeries connections.
MQNLIST	Protects MQSeries namelists.
MQPROC	Protects MQSeries processes.
MQQUEUE	Protects MQSeries queues.
NetView classes	
NETCMDS	Controlling which NetView commands the NetView operator can issue.
NETSPAN	Controlling which NetView commands the NetView operator can issue against the resources in this span.
NVASAPDT	NetView/Access Services.
PTKTVAL	Used by NetView/Access Services Secured Single Signon to store information needed when generating a PassTicket.
RMTOPS	NetView Remote Operations.
RODMMGR	NetView Resource Object Data Manager (RODM).
Network Authentication Service classes	
KERBLINK	Mapping class for user identities of local and foreign principals. ³
REALM	Used to define the local and foreign realms. ³
SMS (DFSMSdfp) classes	
MGMTCLAS	SMS management classes.
STORCLAS	SMS storage classes.
SUBSYSNM	Authorizes a subsystem (such as a particular instance of CICS) to open a VSAM ACB and use VSAM record level sharing (RLS) functions.
Tivoli classes	
ROLE	Specifies the complete list of resources and associated access levels that are required to perform the particular job function this role represents and defines which RACF groups are associated with this role.
TMEADMIN	Maps the user IDs of Tivoli administrators to RACF user IDs.
TSO classes	
ACCTNUM	TSO account numbers.

Table 6. Resource classes for z/OS systems (continued)

Class name	Description
PERFGRP	TSO performance groups.
TSOAUTH	TSO user authorities such as OPER and MOUNT.
TSOPROC	TSO logon procedures.
WebSphere MQ classes	
GMXADMIN	Grouping class for WebSphere MQ administrative options.
GMXNLIST	Grouping class for WebSphere MQ namelists.
GMXPROC	Grouping class for WebSphere MQ processes.
GMXQUEUE	Grouping class for WebSphere MQ queues.
GMXTOPIC	Grouping class for WebSphere MQ topics.
MXADMIN	Protects WebSphere MQ administrative options.
MXNLIST	Protects WebSphere MQ namelists.
MXPROC	Protects WebSphere MQ processes.
MXQUEUE	Protects WebSphere MQ queues.
MXTOPIC	Protects WebSphere MQ topics.
z/OS UNIX classes	
DIRACC	Controls auditing (using SETROPTS LOGOPTIONS) for access checks for read/write access to z/OS UNIX directories. This class need not be active to control auditing. ⁵
DIRSRCH	Controls auditing (using SETROPTS LOGOPTIONS) of z/OS UNIX directory searches. This class need not be active to control auditing. ⁵
FSOBJ	Controls auditing (using SETROPTS LOGOPTIONS) for all access checks for z/OS UNIX file system objects except directory searches. Controls auditing (using SETROPTS AUDIT) of creation and deletion of z/OS UNIX file system objects. This class need not be active to control auditing. ⁵
FSSEC	Controls auditing (using SETROPTS LOGOPTIONS) for changes to the security data (FSP) for z/OS UNIX file system objects. This class need not be active to control auditing. When this class is active, it also controls whether ACLs are used during authorization checks to z/OS UNIX files and directories. ⁵
IPCOBJ	Controls auditing (using SETROPTS LOGOPTIONS) of access checks for interprocess communication (IPC) objects and changes to security information of IPC objects. Controls auditing (using SETROPTS AUDIT) of the creation and deletion of IPC objects. This class need not be active to control auditing. ⁵
PROCACT	Controls auditing (using SETROPTS LOGOPTIONS) of functions that look at data from, or affect the processing of, z/OS UNIX processes. This class need not be active to control auditing. ⁵
PROCESS	Controls auditing (using SETROPTS LOGOPTIONS) of changes to UIDs and GIDs of z/OS UNIX processes. Controls auditing (using SETROPTS AUDIT) of dubbing and undubbing of z/OS UNIX processes. This class need not be active to control auditing. ⁵
UNIXMAP	Contains profiles that are used to map z/OS UNIX UIDs to RACF user IDs and z/OS UNIX GIDs to RACF group names.
UNIXPRIV	Contains profiles that are used to grant z/OS UNIX privileges.

Table 6. Resource classes for z/OS systems (continued)

Class name	Description
Restrictions:	
1.	Do not specify this class name on the GENCMD, GENERIC, and GLOBAL/NOGLOBAL operands of the SETROPTS command.
2.	Do not specify this class name on the GLOBAL operand of SETROPTS or, if you do, the GLOBAL checking is not performed.
3.	Do not specify this class name on the GENCMD and GENERIC operands of the SETROPTS command.
4.	Do not specify this class name with any RACF command. This is a member class associated with a grouping class that has a special use.
5.	Profiles are not allowed in this class.

Supplied resource classes for z/VM systems

Table 7 lists the supplied classes you can use on z/VM systems. These classes are primarily relevant if you share your RACF database with a z/VM system. See restrictions at the end of the table.

Table 7. Resource classes for z/VM systems

Class name	Description
DIRECTRY	Protection of shared file system (SFS) directories.
FACILITY	Miscellaneous uses. Profiles are defined in this class so resource managers (typically elements of z/OS or z/VM) can check a user's access to the profiles when the user takes some action. Examples are the profiles used to control execution of RACDCERT command functions and the profiles used to control privileges in the z/OS UNIX environment. RACF does not document all of the resources used in the FACILITY class by other products. For information on the FACILITY class resources used by a specific product (other than RACF itself), see that product's documentation.
FIELD	Fields in RACF profiles (field-level access checking).
FILE	Protection of shared file system (SFS) files.
GLOBAL	Global access checking. ¹
GMBR	Member class for GLOBAL class. ³
GTERMINL	Terminals whose IDs do not fit into generic profile naming conventions. ¹
PSFMPL	When class is active, PSF/VM performs separator and data page labeling as well as auditing.
PTKTDATA	PassTicket key class.
PTKTVAL	Used by NetView/Access Services Secured Single Signon to store information needed when generating a PassTicket.
RACFVARS	RACF variables. In this class, profile names, which start with & (ampersand), act as RACF variables that can be specified in profile names in other RACF general resource classes.
RVARSMBR	Member class for RACFVARS. ³
SCDMBR	Member class for SECDATA class. ³
SECDATA	Security classification of users and data (security levels and security categories). ¹
SECLABEL	If security labels are used and, if so, their definitions. ²

Table 7. Resource classes for z/VM systems (continued)

Class name	Description
SFSCMD	Controls the use of shared file system (SFS) administrator and operator commands.
TAPEVOL	Tape volumes.
TERMINAL	Terminals (TSO or z/VM). See also GTERMINL class.
VMATCH	Alternate user IDs.
VMBR	Member class for VMEVENT class. ³
VMCMD	Certain CP commands and other requests on z/VM.
VMEVENT	Auditing and controlling security-related events (called z/VM events) on z/VM systems.
VMLAN	Controls access to z/VM guest LANs and virtual switches.
VMMAC	Used in conjunction with the SECLABEL class to provide security label authorization for some z/VM events. ⁴
VMMDISK	z/VM minidisks.
VMNODE	RSCS nodes.
VMRDR	z/VM unit record devices (virtual reader, virtual printer, and virtual punch).
VMSEGMT	Restricted segments, which can be named saved segments (NSS) and discontinuous saved segments (DCSS).
VXMBR	Member class for VMXEVENT class. ³
VMXEVENT	Auditing and controlling security-related events (called z/VM events) on z/VM systems.
VMPOSIX	Contains profiles used by OpenExtensions for z/VM.
WRITER	z/VM print devices.

Restrictions:

1. Do not specify this class name on the GENCMD, GENERIC, and GLOBAL/NOGLOBAL operands of the SETROPTS command.
2. Do not specify this class name on the GLOBAL operand of SETROPTS or, if you do, the GLOBAL checking is not performed.
3. Do not specify this class name with any RACF command. This is a member class associated with a grouping class that has a special use.
4. Profiles are not allowed in this class.

Appendix B. Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in z/OS enable users to:

- Use assistive technologies such as screen readers and screen magnifier software
- Operate specific or equivalent features using only the keyboard
- Customize display attributes such as color, contrast, and font size

Using assistive technologies

Assistive technology products, such as screen readers, function with the user interfaces found in z/OS. Consult the assistive technology documentation for specific information when using such products to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. Refer to *z/OS TSO/E Primer*, *z/OS TSO/E User's Guide*, and *z/OS ISPF User's Guide Vol I* for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

z/OS information

z/OS information is accessible using screen readers with the BookServer/Library Server versions of z/OS books in the Internet library at:

<http://www.ibm.com/systems/z/os/zos/bkserv/>

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.

COPYRIGHT LICENSE:

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

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.



Policy for unsupported hardware

Various z/OS elements, such as DFSMS™, HCD, JES2, JES3, and MVS, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for

service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>.

Adobe is either a registered trademark or trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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

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

Index

Special characters

- * (asterisk)
 - as generic character in profile names 60
- ** (double asterisk)
 - as generic character in profile names 60
- % (percent sign)
 - as generic character in profile names 59

A

- access attempts
 - recording and reporting 3
- access authority
 - denying access to data sets 75
 - denying access to general resources 82
 - for data sets 85
 - granting access to data sets 74
 - granting access to general resources 81
- ACCESS COUNT field
 - in LISTDSD output 68
- ACCESS field
 - in LISTDSD output 68
- access list
 - data set profile
 - changing 74, 75
 - displaying 64
 - description 2
 - general resource profile
 - changing 81, 82
- accessibility 101
- ACCTNUM class
 - description 97
- ACICSPCT class
 - description 94
- ADDSD command
 - creating a profile
 - discrete 58
 - generic 59
- administration, RACF
 - classroom courses xii
- ADSP (automatic data set protection) attribute
 - user attribute 19
- ADSP (automatic data set protection) group-level attribute
 - group-level attribute 22
- AIMS class
 - description 96
- ALCSAUTH class
 - description 91
- allowing another user to submit your jobs 50
- ALTDSD command
 - changing the UACC (universal access authority) 73
- ALTER access authority 85, 86
- ALTER COUNT field
 - in LISTDSD output 68
- APPCLU class
 - description 91
- APPCPORT class
 - description 91
- APPCSERV class
 - description 91
- APPCSI class
 - description 91
- APPCTP class
 - description 91
- APPL class
 - description 91
- approving user ID association 53
- association, user ID
 - information in user profile 39
- asterisk (*)
 - as generic character in profile names 60
- AT keyword
 - using on RACF commands 10
- attribute
 - connect 22
 - group-level 22
 - system-wide, of user 18
- ATTRIBUTES field
 - in LISTUSER output 18
- AUDITING field
 - in LISTDSD output 67
- AUDITOR attribute 18
- AUDITOR group-level attribute 22
- AUTH field
 - in LISTUSER output 20
- authority
 - allowing another user to submit your jobs 50
 - as a member of a group 20
 - group 20
 - resource access 86
 - UACC (universal access authority)
 - access authority for data sets 85
 - access authority for general resources 86
 - data set protection (discrete profile) 57
 - data set protection (generic profile) 62
- automatic command direction 12
- automatic data set protection (ADSP)
 - group-level attribute 22
- automatic data set protection (ADSP) attribute
 - user attribute 19
- automatic direction of application updates 90
 - and ADSP attribute 19, 22
 - and choosing discrete or generic profiles 56
- automatic password direction 46

B

- BCICSPCT class
 - description 94

C

- CACHECLS class
 - description 91
- CATEGORIES field
 - in LISTDSD output 67
- CATEGORY-AUTHORIZATION field
 - in LISTUSER output 20
- CBIND class
 - description 91
- CCICSCMD class
 - description 94
- CDT class
 - description 91
- certificate, digital
 - automatic registration of 41
 - listing information for 41
- CFIELD class
 - description 91
- CICS
 - general resource classes 94
 - information in user profile 24
 - segment in user profile 24
- CIMS class
 - description 96
- CLASS AUTHORIZATIONS field
 - in LISTUSER output 19
- class descriptor table (CDT)
 - supplied classes for z/OS systems 91
 - supplied classes for z/VM systems 99
- CLASS field
 - in LISTDSD output 68
- classes
 - names of supplied general resource classes for z/OS 91
 - names of supplied general resource classes for z/VM 99
- classroom courses, RACF xii
- CLAUTH (class authority group-level) attribute 22
- CLAUTH (class authority) attribute 19
- command
 - abbreviating 10
 - escaping from prompt sequence 10
 - general user tasks 7
 - online help for 10
 - performing security tasks with 7
 - processing on another node or user ID 10
- command direction 10, 13
 - automatic 12
- CONNECT-ATTRIBUTES field
 - in LISTUSER output 22
- CONNECT-DATE field
 - in LISTUSER output 21
- CONNECT-OWNER field
 - in LISTUSER output 21
- CONNECTS field
 - in LISTUSER output 21
- CONSOLE class
 - description 91
- CONTROL access authority 85, 86
- CONTROL COUNT field
 - in LISTDSD output 68

- courses about RACF xii
- CPSMOBJ class
 - description 94
- CPSMXMP class
 - description 94
- CREATED field
 - in LISTUSER output 17
- CREATION DATE field
 - in LISTDSD output 67
- CREATION GROUP field
 - in LISTDSD output 67
- CRYPTOZ class
 - brief description 96
- CSDATA segment in user profile 25
- CSFKEYS class
 - description 96
- CSFSERV class
 - description 96
- custom fields
 - information in user profile 25

D

- DASDVOL class
 - description 91
- data set
 - access authority for 85
 - determining how protected 64
 - RRSFLIST 11
 - VSAM 59
- data set profile
 - changing access list 74
 - changing UACC (universal access authority) 73
 - deleting 69
 - denying access to data sets 75
 - description 55
 - determining the protection status of a data set 64
 - discrete 57
 - generic 59
 - listing 64
 - listing ones you own 69
 - permitting access to a data set 74
 - UACC (universal access authority)
 - description 85
 - when changes take effect 89
- DATASET TYPE field
 - in LISTDSD output 67
- DB2
 - general resource classes 95
- DCE
 - general resource class 95
 - information in user profile 26
 - segment in user profile 26
 - segment information
 - example 27
- DCICSDCT class
 - description 94
- default group
 - logging on to a group other than 47
- default security label
 - logging on with a security label other than 48

- DEFAULT-GROUP field
 - in LISTUSER output 18
- defining user ID associations 52
- DELDSD command 69
- deleting
 - data set profile 69
 - user ID association 54
- denying access
 - to data sets 75
 - to general resources 82
- DEVICES class
 - description 92
- DFP
 - segment information
 - example 28
- DFP INFORMATION field
 - in LISTDSD output 69
- DFP segment in user profile 28
- DFSMSdfp
 - general resource classes 97
 - information in user profile 28
- digital certificate
 - automatic registration of 41
 - listing information for 41
- digital key ring
 - listing information for 41
- DIGTCERT class
 - description 92
- DIGTCRIT class
 - description 92
- DIGTNMAP class
 - description 92
- DIGTRING class
 - description 92
- DIMS class
 - description 96
- DIRACC class
 - description 98
- DIRAUTH class
 - description 92
- DIRECTRY class
 - description 99
- DIRSRCH class
 - description 98
- disability 101
- discrete profile
 - deleting 69
 - for a data set 55
 - for a data set, creating 57
- displaying date last updated 18
- displaying how long it is valid 18
- displaying whether you have one 19
- distributed identity information
 - viewing 27
- DLFCLASS class
 - description 92
- double asterisk (**)
- as generic character in profile names 60
- DSNADM class
 - description 95

- DSNR class
 - description 95

E

- ECICSDCT class
 - description 94
- EIM
 - general resource class 95
 - information in user profile 28
- EIM segment in user profile 28
- EJBROLE class
 - description 96
- enhanced generic naming
 - for data set profile 88
- Enterprise Identity Mapping
 - general resource class 95
 - information in user profile 28
- Enterprise Java Beans
 - general resource classes 96
- ENTITY NAME field
 - in LISTDSD output 68
- ERASE field
 - in LISTDSD output 66
- erase-on-scratch
 - determining for a data set profile 66
 - specifying for a data set profile 62
- EXECUTE access authority 86
- execution user 50

F

- FACILITY class
 - description 92, 99
- FCICSFCT class
 - description 94
- FIELD class
 - description 92, 99
- FILE class
 - description 99
- FIMS class
 - description 96
- FSOBJ class
 - description 98
- FSSEC class
 - description 98
- fully-qualified generic profile 56

G

- GCICSTRN class
 - description 94
- GCPSMOBJ class
 - description 94
- GCSFKEYS class
 - description 96
- GDASDVOL class
 - description 92
- GDSNBP class
 - description 95

- GDSNCL class
 - description 95
- GDSNDB class
 - description 95
- GDSNJR class
 - description 95
- GDSNPK class
 - description 95
- GDSNPN class
 - description 95
- GDSNSC class
 - description 95
- GDSNSG class
 - description 95
- GDSNSM class
 - description 95
- GDSNSP class
 - description 95
- GDSNSQ class
 - description 95
- GDSNTB class
 - description 95
- GDSNTS class
 - description 95
- GDSNUF class
 - description 95
- GDSNUT class
 - description 95
- GEJBROLE class
 - description 96
- general resource class 95
 - product use of
 - CICS 94
 - DB2 95
 - DCE 95
 - DFSMSdfp 97
 - EIM 95
 - Enterprise Identity Mapping 95
 - Enterprise Java Beans 96
 - ICSF 96
 - IMS 96
 - Infoprint Server 96
 - Information/Management 96
 - LFS/ESA 96
 - License Manager 96
 - Lotus Notes for z/OS 97
 - MQSeries 97
 - NetView 97
 - Novell Directory Services for OS/390 97
 - Security Server Network Authentication Service 97
 - SMS 97
 - Tivoli 97
 - Tivoli Service Desk 96
 - TSO 97
 - WebSphere MQ 98
 - z/OS UNIX 98
 - supplied for z/OS 91
 - supplied for z/VM 99
- general resource profile
 - denying an individual or group the use of 82
 - general resource profile (*continued*)
 - listing the contents of 80
 - permitting an individual or group to 81
 - searching for names 79
 - generic character (*, **, and %)
 - in profile names 59, 60
 - generic profile
 - DATASET class
 - enhanced generic naming active 88
 - enhanced generic naming inactive 86
 - deleting 69
 - for a data set 56
 - for a data set, creating 59
 - fully-qualified 56
 - GIMS class
 - description 96
 - GINFOMAN class
 - description 96
 - GLOBAL class
 - description 92, 99
 - GMBR class
 - description 92, 99
 - GMQADMIN class
 - description 97
 - GMQNLIST class
 - description 97
 - GMQPROC class
 - description 97
 - GMQQUEUE class
 - description 97
 - GMXADMIN
 - description 98
 - GMXNLIST
 - description 98
 - GMXPROC
 - description 98
 - GMXQUEUE
 - description 98
 - GMXTOPIC
 - description 98
 - group
 - description of 2
 - logging on to 47
 - your authority as a member 20
 - GROUP field
 - in LISTUSER output 20
 - group-level attribute
 - in LISTUSER output 22
 - GRPACC (group access) attribute
 - for user 19
 - group-level 22
 - GSDSF class
 - description 92
 - GTERMINL class
 - description 92, 99
 - GXCFSKEY class
 - description 96
 - GXFACILI class
 - description 92

H

- HCICSFCT class
 - description 94
- help
 - for commands 10
 - for RACF messages 12
- HIMS class
 - description 96

I

- ICSF (Integrated Cryptographic Service Facility)
 - general resource classes 96
- ID field
 - in LISTDSD output 68
- ID(*) in an access list 75
- identity, distributed 27
- IDIDMAP class 27
- IIMS class
 - description 96
- ILMADMIN class
 - description 97
- IMS (Information Management System)
 - general resource classes 96
- INFOMAN class
 - description 96
- Infoprint Server
 - general resource class 96
- Information/Management
 - general resource classes 96
- INSTALLATION DATA field
 - in LISTDSD output 67
- INSTALLATION-DATA field
 - in LISTUSER output 19
- installation-defined data
 - information in user profile 25
- IPCOBJ class
 - description 98

J

- JAVA class
 - description 96
- JCICSJCT class
 - description 94
- JESINPUT class
 - description 92
- JESJOBS class
 - description 92
- JESSPOOL class
 - description 92
- JIMS class
 - description 96

K

- KCICSJCT class
 - description 94
- KERB segment in user profile 29

- Kerberos
 - information in user profile 29
- KERBLINK class
 - description 97
- key ring, digital
 - listing information for 41
- keyboard 101
- keys
 - PA1 10
- keywords on RACF commands
 - AT 10

L

- LAN File Services/ESA (LFS/ESA)
 - See LFS/ESA (LAN File Services/ESA)
- LANGUAGE
 - segment in user profile 30
- language information in user profile 30
- LAST CHANGE DATE field
 - in LISTDSD output 67
- LAST REFERENCE DATE field
 - in LISTDSD output 67
- LAST-ACCESS field
 - in LISTUSER output 19
- LAST-CONNECT field
 - in LISTUSER output 22
- LEVEL field
 - in LISTDSD output 66
- LFS/ESA (LAN File Services/ESA)
 - general resource class 96
- LFSCCLASS class
 - description 96
- License Manager
 - general resource class 96
- LIMS class
 - description 96
- LISTDSD command
 - determining protection status of data set 64
 - determining UACC (universal access authority) 73
 - output 64
- LISTUSER command
 - examples 23
 - output 16
- LNOTES segment in user profile 31
- logging on
 - to a group other than your default group 47
 - to TSO/E 15
 - with a security label other than your default security label 48
- LOGON ALLOWED field
 - in LISTUSER output 19
- Lotus Notes
 - information in user profile 31
- Lotus Notes for z/OS
 - general resource class 97

M

- mainframe
 - education xiv

- managed user ID association
 - approving 53
 - defining 53
 - deleting 54
 - description 52
 - rejecting 54
- MCICSPPT class
 - description 94
- MDSNBP class
 - description 95
- MDSNCL class
 - description 95
- MDSNDB class
 - description 95
- MDSNJR class
 - description 95
- MDSNPK class
 - description 95
- MDSNPN class
 - description 95
- MDSNSC class
 - description 95
- MDSNSG class
 - description 95
- MDSNSM class
 - description 95
- MDSNSP class
 - description 95
- MDSNSQ class
 - description 95
- MDSNTB class
 - description 95
- MDSNTS class
 - description 95
- MDSNUF class
 - description 95
- MDSNUT class
 - description 95
- messages
 - notification, from command direction and password synchronization 13
- messages, RACF
 - getting help for 12
- MGMTCLAS class
 - description 97
- MIMS class
 - description 96
- MODEL-NAME field
 - in LISTUSER output 19
- MQADMIN class
 - description 97
- MQCMDS class
 - description 97
- MQCONN class
 - description 97
- MQNLIST class
 - description 97
- MQPROC class
 - description 97
- MQQUEUE class
 - description 97

- MQSeries
 - general resource classes 97
- MXADMIN
 - description 98
- MXNLIST
 - description 98
- MXPROC
 - description 98
- MXQUEUE
 - description 98
- MXTOPIC
 - description 98

N

- NAME field
 - in LISTUSER output 17
- NCICSPPT class
 - description 94
- NDSLINK class
 - description 97
- NETCMDS class
 - description 97
- NETSPAN class
 - description 97
- NetView
 - general resource classes 97
 - information in user profile 31
- NETVIEW segment in user profile 31
- Network Authentication Service
 - general resource classes 97
 - information in user profile 29
- NODES class
 - description 93
- NODMBR class
 - description 93
- NONE access authority 85, 86
- NONE group-level attribute 22
- NOTELINK class
 - description 97
- Notices 103
- notification messages from command direction and password synchronization 13
- NOTIFY field
 - in LISTDSD output 67
- Novell Directory Services for OS/390
 - general resource class 97
- NVASAPDT class
 - description 97

O

- OIMS class
 - description 96
- OMVS segment in user profile 35
- online help
 - commands 10
 - for RACF messages 12
- OpenExtensions
 - information in user profile 33

- operand on command
 - abbreviating 10
- OPERATIONS attribute 18
- OPERATIONS group-level attribute 22
- operator information for extended MCS console session
 - in user profile 33
- OPERCMD5 class
 - description 93
- OPERPARM segment in user profile 33
- output format
 - automatic direction of application updates 90
- OVM segment in user profile 33
- OWNER field
 - in LISTDSD output 66
 - in LISTUSER output 17

P

- PA1 key 10
- panels, RACF 5
- PASS-INTERVAL field
 - in LISTUSER output 18
- PASSDATE field
 - in LISTUSER output 18
- PASSPHRASE attribute 19
- password 18
 - automatic password direction 46
 - changing
 - using commands 43
 - using panels 15
 - synchronizing 45
- PASSWORD ENVELOPED field
 - in LISTUSER output 18
- password phrase 18, 19
 - automatic password direction 46
 - changing 44
 - description 1
 - synchronizing 45
- password synchronization 13
 - are you defined for 39
 - defining a user ID association with 52
- PCICSPSB class
 - description 94
- peer user ID association
 - approving 53
 - defining with password synchronization 52
 - defining without password synchronization 52
 - deleting 54
 - description 52
 - rejecting 54
- percent sign (%)
 - as generic character in profile names 59
- PERFGRP class
 - description 98
- PERMIT command
 - allowing access to data sets 74
 - allowing access to general resources 81
 - denying access to data sets 75
 - denying access to general resources 82
- permitting access
 - to data sets 74

- permitting access (*continued*)
 - to general resources 81
- PHRASE ENVELOPED field
 - in LISTUSER output 18
- PHRASEDATE field
 - in LISTUSER output 18
- PIMS class
 - description 96
- PMBR class
 - description 93
- Print Services Facility (PSF) for z/OS
 - PSFMPL, general resource class 93
- PRINTSRV class
 - description 96
- privileges
 - group authority 20
- PROCACT class
 - description 98
- PROCESS class
 - description 98
- profile
 - data set
 - discrete 55
 - fully-qualified generic 56
 - generic 56
 - listing ones you own 69
 - defining with enhanced generic naming 88
 - description of 2
 - group 2
 - resource 2
 - user 2
- PROGRAM class
 - description 93
- prompt sequence
 - escaping from 10
- PROPCNTL class
 - description 93
- PROTECTALL(FAILURES) SETROPTS option 69
- protected resources
 - authorizing users to access 2
- protecting
 - data sets
 - deleting a data set profile 69
 - with discrete profiles 57
 - with generic profiles 59
 - determining the protection of a data set 64
 - general resources 79
- PSFMPL class
 - description 93, 99
- PTKTDATA class
 - description 93, 99
- PTKTVAL class
 - description 97, 99
- publications
 - on CD-ROM and DVD xii
 - softcopy xii

Q

- QCICSPSB class
 - description 94

QIMS class
description 96

R

RACDCERT command
using to list digital certificate information 41
using to list digital key ring information 41

RACF
publications
on CD-ROM and DVD xii
softcopy xii

RACF commands
automatic direction 12
directing 10
general user tasks 7
performing security tasks with 7

RACFEVNT class
description 93

RACFHC class
description 93

RACFVARS class
description 93, 99

RACGLIST class
description 93

RACHCMBR class
description 93

RACLINK command
APPROVE keyword 53
UNDEFINE keyword 54
using to list user ID associations 40

RACMAP command
viewing your distributed identity mappings 27

RAUDITX class
description 95

RCICSRES class
description 94

RDATALIB class
description 93

READ access authority 85, 86

READ COUNT field
in LISTDSD output 68

REALM class
description 97

registering digital certificates 41

rejecting
user ID association 54

remote sharing
See RRSF (RACF remote sharing facility)

resource
description of 2
protecting 2, 79
types of 79

resource access authority
UACC (universal access authority)
access authority for data sets 85
access authority for general resources 86
data set protection (discrete profile) 57
data set protection (generic profile) 62

resource profile
changing the access list 81

resource profile (*continued*)
denying access to a general resource 82
permitting access to a general resource 81

RESOWNER field
in LISTDSD output 69

RESUME DATE field
in LISTUSER output 19

RESUME DATE field, group-level
in LISTUSER output 23

REVOKE attribute 19

REVOKE DATE field
in LISTUSER output 19

REVOKE DATE field, group-level
in LISTUSER output 23

REVOKE group-level attribute 22

RIMS class
description 96

RMTOPS class
description 97

RODMMGR class
description 97

ROLE class
description 97

RRSF (RACF remote sharing facility) 10
automatic command direction 12
automatic password direction 46
command direction 10
output 11, 46
RRSFLIST user data set 11, 46

RRSFDATA class
description 93

RRSFLIST data set 11

RRSFLIST user data set 46

RVARSMBR class
description 93, 99

S

SCDMBR class
description 93, 99

SCICSTST class
description 94

SDSF (System Display and Search Facility)
general resource class 93

SDSF class
description 93

SEARCH command
finding out what data set profiles you own 69

SECDATA class
description 93, 99

SECLABEL class
description 93, 99

SECLMBR class
description 93

security label
logging on with 48

security tasks
performing
using RACF commands 7
using RACF panels 5

- security topics for RACF
 - classroom courses xii
- SECURITY-LABEL field
 - in LISTDSD output 67
 - in LISTUSER output 20
- SECURITY-LEVEL field
 - in LISTDSD output 67
 - in LISTUSER output 20
- seeing and suppressing notification messages from 13
- SERVAUTH class
 - description 93
- SERVER class
 - description 93
- SFSCMD class
 - description 100
- shortcut keys 101
- SIMS class
 - description 96
- SMESSAGE class
 - description 94
- SMS (Storage Management Subsystems)
 - general resource classes 97
- SOMDOBJ class
 - description 94
- SPECIAL attribute 18
- SPECIAL group-level attribute 22
- STARTED class
 - description 94
- STORCLAS class
 - description 97
- submitting jobs
 - allowing another user to submit yours 50
 - surrogate user 50
- SUBSYSNM class
 - description 97
- SURROGAT class
 - description 94
- surrogate user 50
- synchronizing passwords and password phrases 45
- SYSMVIEW class
 - description 94
- System Display and Search Facility (SDSF)
 - See SDSF (System Display and Search Facility)

T

- TAPEVOL class
 - description 94, 100
- TCICSTRN class
 - description 94
- TEMPDSN class
 - description 94
- TERMINAL class
 - description 94, 100
- TIMS class
 - description 96
- Tivoli
 - general resource class 97
- Tivoli Service Desk
 - general resource classes 96

- TMEADMIN class
 - description 97
- TSO segment in user profile 37
- TSO/E
 - command abbreviations 10
 - escaping from command prompts 10
 - general resource classes 97
 - information in user profile 37
 - logon 15
- TSOAUTH class
 - description 98
- TSOPROC class
 - description 98

U

- UACC (universal access authority) 16, 86
 - ALTER 58, 61
 - changing the UACC of a data set 73
 - CONTROL 57, 61
 - description 21, 57
 - determining 73
 - EXECUTE 58, 62
 - field description 62
 - for data sets 85
 - NONE 57, 61
 - READ 57, 61
 - UPDATE 57, 61
- UACC field
 - in LISTUSER output 21
- UCICSTST class
 - description 94
- UIMS class
 - description 96
- UNIT field
 - in LISTDSD output 67
- universal access authority (UACC)
 - See also UACC (universal access authority)
 - for data sets 85
- UNIVERSAL ACCESS field
 - in LISTDSD output 66
- UNIXMAP class
 - description 98
- UNIXPRIV class
 - description 98
- UPDATE access authority 85, 86
- UPDATE COUNT field
 - in LISTDSD output 68
- user
 - allowing access to data sets 74
 - attributes 18
 - authorizing access to protected resources 2
 - execution 50
 - identifying and verifying 1
 - permitting access to general resources 81
 - profile, contents of 16
 - RACF information about 17
 - surrogate 50
- USER field
 - in LISTUSER output 17

- user ID association
 - approving 53
 - information in user profile 39
 - listing 40
- user ID associations
 - defining 52
 - deleting 54
 - description 51
 - rejecting 54

V

- VCICSCMD class
 - description 95
- VM
 - OpenExtensions information in user profile 33
 - OVN segment in user profile 33
- VMATCH class
 - description 100
- VMBR class
 - description 100
- VMCMD class
 - description 100
- VMEVENT class
 - description 100
- VMLAN class
 - description 100
- VMMAC class
 - description 100
- VMMDISK class
 - description 100
- VMNODE class
 - description 100
- VMPOSIX class
 - description 100
- VMRDR class
 - description 100
- VMSEGMT class
 - description 100
- VMXEVENT class
 - description 100
- VOLUME ON WHICH THE DATASET RESIDES field
 - in LISTDSD output 67
- VSAM data set
 - protecting 57, 59
- VTAM (Virtual Telecommunications Access Method)
 - general resource class 94
- VTAMAPPL class
 - description 94
- VXMBR class
 - description 100

W

- WARNING field
 - in LISTDSD output 66
- WCICSRES class
 - description 95
- WebSphere MQ
 - general resource classes 98

- WIMS class
 - description 96
- work attribute information in user profile 38
- WORKATTR segment in user profile 38
- WRITER class
 - description 94, 100

X

- XCSFKEY class
 - description 96
- XFACILIT class
 - description 94

Y

- YOUR ACCESS field
 - in LISTDSD output 67

Z

- z/OS Basic Skills information center xiv
- z/OS UNIX
 - general resource classes 98
 - information in user profile 35
- z/VM
 - OpenExtensions information in user profile 33

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

**z/OS
Security Server RACF
General User's Guide**

Publication No. SA22-7685-05

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Submit your comments using one of these channels:

- Send your comments to the address on the reverse side of this form.
- Send your comments via e-mail to: mhvrcfs@us.ibm.com

If you would like a response from IBM, please fill in the following information:

Name

Address

Company or Organization

Phone No.

E-mail address



Fold and Tape

Please do not staple

Fold and Tape



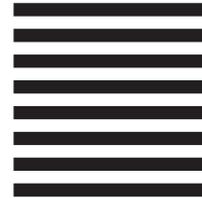
NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

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

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
MHVRCFS, Mail Station P181
2455 South Road
Poughkeepsie, NY
12601-5400



Fold and Tape

Please do not staple

Fold and Tape



Program Number: 5694-A01

Printed in USA

SA22-7685-05

