z/OS

Security Server RACF General User's Guide

Version 2 Release 2

SA23-2298-02

Note
Before using this information and the product it supports, read the information in "Notices" on page 101.

This edition applies to Version 2 Release 2 of z/OS (5650-ZOS) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 1994, 2016.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

© Copyright IBM Corp. 1994, 2016

Tables

© Copyright IBM Corp. 1994, 2016

Figures

© Copyright IBM Corp. 1994, 2016

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, including 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 topic 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 17 through Chapter 9, "Protecting general resources," on page 83. 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 89 as a reference for information such as access authority, naming conventions, and RACF-defined classes.

© Copyright IBM Corp. 1994, 2016

Where to find more information

When possible, this information uses cross-document links that go directly to the topic in reference using shortened versions of the document title. For complete titles and order numbers of the documents for all products that are part of z/OS, see *z/OS V2R2 Information Roadmap*.

To find the complete z/OS library, including the z/OS Knowledge Center, see IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSLTBW/welcome).

RACF courses

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

ES191 *Basics of z/OS RACF Administration*

BE870 *Effective RACF Administration*

ES885 *Exploiting the Advanced Features of RACF*

IBM® provides various 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)

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.

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 that are 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, 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 go to the RACF home page on the World Wide Web using this address:

  `http://www.ibm.com/systems/z/os/zos/features/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 "Resources" file tab, then select "Downloads" from the list, or go to http://www-03.ibm.com/systems/z/os/zos/features/racf/goodies.html.

  The code is also available from 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 is posted on the RACF-L discussion list 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 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.

How to send your comments to IBM

We appreciate your input on this documentation. Please provide us with any feedback that you have, including comments on the clarity, accuracy, or completeness of the information.

Use one of the following methods to send your comments:

Important: If your comment regards a technical problem, see instead "If you have a technical problem."

- Send an email to mhvrcfs@us.ibm.com.
- Send an email from the "Contact us" web page for z/OS (http://www.ibm.com/systems/z/os/zos/webqs.html).

Include the following information:

- Your name and address
- Your email address
- Your phone or fax number
- The publication title and order number:
  z/OS Security Server RACF General User's Guide
  SA23-2298-02
- The topic and page number or URL of the specific information to which your comment relates
- The text of your comment.

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

IBM or any other organizations use the personal information that you supply to contact you only about the issues that you submit.

If you have a technical problem

Do not use the feedback methods that are listed for sending comments. Instead, take one or more of the following actions:

- Visit the IBM Support Portal (support.ibm.com).
- Contact your IBM service representative.
- Call IBM technical support.

© Copyright IBM Corp. 1994, 2016

Summary of changes

Summary of changes for z/OS Version 2 Release 2 (V2R2) as updated June 2016

The following changes are made to z/OS Version 2 Release 2 (V2R2).

New

- Added information about IBM Multi-Factor Authentication. See "Identifying and verifying users" on page 1 for more information.
- Added information about the ASSIZEMAX value limits in "Finding out what z/OS UNIX information RACF has about you" on page 38.

Changed

There is no changed information in this edition.

Summary of changes for z/OS Version 2 Release 2 (V2R2)

The following changes are made to z/OS Version 2 Release 2 (V2R2).

New

- "Changing your password" on page 47 has new information about special characters.
- The NOPASSWORD attribute is added to "Understanding the information RACF has about you as a user" on page 19.

Changed

There is no changed information in this edition.

z/OS Version 2 Release 1 summary of changes

See the following publications for all enhancements to z/OS Version 2 Release 1 (V2R1):

- *z/OS Migration*
- *z/OS Planning for Installation*
- *z/OS Summary of Message and Interface Changes*
- *z/OS Introduction and Release Guide*

© Copyright IBM Corp. 1994, 2016

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 that you want to use. It does so by requiring a user identification, the user ID, which is a unique identification string. RACF then verifies that you are the user you say that 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 through digital certificates or Kerberos. When you access these applications, you might not need to enter a user ID and password.

In addition to a password, you can have a password phrase that 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.

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 47 for information about 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 to 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 about how to do this, see "Changing your password phrase" on page 48.

You can be required to authenticate with multiple authentication factors instead of a password or password phrase. In this case, what you enter when you log on is

© Copyright IBM Corp. 1994, 2016

determined by IBM Multi-Factor Authentication for z/OS. For example, you might be required to enter an RSA SecurID token code and PIN. See *IBM Multi-Factor Authentication for z/OS User's Guide* for more information.

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 that is 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 V2R2.0 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 that is 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 and 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 that 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.

Note:

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.

© Copyright IBM Corp. 1994, 2016

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`	"Finding out how you are defined to RACF" on page 18
Find out what CICS® information RACF has about you	`LISTUSER` *`your-userid`* `CICS NORACF`	"Finding out what CICS information RACF has about you" on page 26
Find out what custom field information RACF has about you	`LISTUSER` *`your-userid`* `CSDATA NORACF`	"Finding out what custom field information RACF has about you" on page 27
Find out what DCE information RACF has about you	`LISTUSER` *`your-userid`* `DCE NORACF`	"Finding out what DCE information RACF has about you" on page 28
Find out what distributed identity information RACF has about you	`RACMAP`	"Finding out what distributed identity information RACF has about you" on page 29
Find out what DFSMSdfp information RACF has about you	`LISTUSER` *`your-userid`* `DFP NORACF`	"Finding out what DFSMSdfp information RACF has about you" on page 30
Find out what EIM information RACF has about you	`LISTUSER` *`your-userid`* `EIM NORACF`	"Finding out what EIM information RACF has about you" on page 31

© Copyright IBM Corp. 1994, 2016

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

Task	Command	Where described
Find out what Kerberos information RACF has about you	`LISTUSER your-userid KERB NORACF`	"Finding out what Kerberos information RACF has about you" on page 31
Find out what language information RACF has about you	`LISTUSER your-userid LANGUAGE NORACF`	"Finding out what language information RACF has about you" on page 32
Find out what information related to Lotus® Notes® RACF has about you	`LISTUSER your-userid LNOTES NORACF`	"Finding out what Lotus Notes information RACF has about you" on page 33
Find out what NetView® information RACF has about you	`LISTUSER your-userid NETVIEW NORACF`	"Finding out what NetView information RACF has about you" on page 34
Find out what OPERPARM information RACF has about you	`LISTUSER your-userid OPERPARM NORACF`	"Finding out what OPERPARM information RACF has about you" on page 36
Find out what OpenExtensions information RACF has about you	`LISTUSER your-userid OVM NORACF`	"Finding out what OpenExtensions information RACF has about you" on page 35
Find out what TSO/E information RACF has about you	`LISTUSER your-userid TSO NORACF`	"Finding out what TSO/E information RACF has about you" on page 40
Find out what WORKATTR information RACF has about you	`LISTUSER your-userid WORKATTR NORACF`	"Finding out what WORKATTR information RACF has about you" on page 41
Find out what z/OS UNIX System Services (z/OS UNIX) information RACF has about you	`LISTUSER your-userid OMVS NORACF`	"Finding out what z/OS UNIX information RACF has about you" on page 38
List all of your user ID associations	`RACLINK LIST`	"Finding out what user ID associations are defined for you" on page 43
List all of your user ID associations with a specific node, user ID, or both	`RACLINK LIST(node.userid)`	"Finding out what user ID associations are defined for you" on page 43
List all of your digital certificates	`RACDCERT LIST`	"Listing your digital certificate information" on page 44

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

Task	Command	Where described
List all of your digital certificate key rings	`RACDCERT LISTRING(*)`	"Listing your digital certificate information" on page 44
Change your password (*pw*)	`PASSWORD PASSWORD(current-pw new-pw)`	"Changing your password" on page 47

Change your password and password phrase interval	`PASSWORD INTERVAL(interval-you-want)`
	or
	`PHRASE INTERVAL(interval-you-want)`
		"Changing your password" on page 47

Change your password phrase (*pp*)	`PASSWORD PHRASE (current-pp new-pp)`
	or
	`PHRASE PHRASE (current-pp new-pp)`
		"Changing your password phrase" on page 48

Log on to a group other than your default group	`LOGON userid GROUP(groupname)` **Note:** The LOGON command is a TSO command, not a RACF command.	"Logging on to TSO/E with a group other than your default group" on page 52

Log on with a security label other than your default security label	`LOGON userid`
	`  SECLABEL(security-label)`
	
	Note: The LOGON command is a TSO command, not a RACF command.
		"Logging on with a security label other than your default security label" on page 53

Allow another user to submit your jobs	`PERMIT CLASS(SURROGAT) userid.SUBMIT`
	`  ID(surrogate-userid)`
	`  ACCESS(READ)`
		"Allowing another user to submit your jobs" on page 54

Enable your user IDs to have their passwords become synchronized as they are changed	`RACLINK`
	`  DEFINE(target-node.target-userid)`
	`  PEER(PWSYNC)`
	
	`RACLINK APPROVE(node.userid)`
	
	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.
		"Defining a peer user ID association with password synchronization" on page 56

Define a peer user ID association with password synchronization	`RACLINK`
	`  DEFINE(target-node.target-userid)`
	`  PEER(PWSYNC)`
		"Defining a peer user ID association with password synchronization" on page 56

Define a peer user ID association without password synchronization	`RACLINK`
	`  DEFINE(target-node.target-userid)`
	`  PEER(NOPWSYNC)`
		"Defining a peer user ID association with password synchronization" on page 56

Define a managed user ID association	`RACLINK`
	`  DEFINE(target-node.target-userid)`
	`  MANAGED`
		"Defining a managed user ID association" on page 57

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

Task	Command	Where described
Approve a user ID association	`RACLINK APPROVE(node.userid)`	"Approving user ID associations" on page 58
Delete a pending or existing user ID association	`RACLINK UNDEFINE(node.userid)`	"Deleting user ID associations" on page 58
Create a discrete profile to protect a cataloged data set	`ADDSD 'dataset-name'` `  UACC(access-authority)`	"Creating a discrete profile to protect a data set" on page 61

Create a discrete profile to protect an uncataloged data set	`ADDSD 'dataset-name' UNIT(type)`
	`  VOLUME(volume-serial)`
	`  UACC(access-authority)`
		"Creating a discrete profile to protect a data set" on page 61

Create a generic profile to protect a data set	`ADDSD`
	`  'dataset-name-with-generic-char.'`
	`  UACC(access-authority)`
	
	or
	
	`ADDSD 'dataset-name'`
	`  UACC(access-authority) GENERIC`
		"Creating a generic profile to protect a data set" on page 64

Find out how a data set is protected	`LISTDSD DATASET('dataset-name') ALL`
	
	or
	
	`LISTDSD DATASET('dataset-name') ALL`
	`  GENERIC`
		"Finding out how a data set is protected" on page 68

Check what data set profiles you have	`SEARCH`	"Finding out what data set profiles you have" on page 74
Delete a data set profile	`DELDSD 'profile-name'`	"Deleting a data set profile" on page 74
Change a data set's universal access authority	`ALTDSD 'profile-name'` `  UACC(access-authority)`	"Changing the universal access authority to a data set" on page 79

Permit an individual or a group to use a data set	`PERMIT 'profile-name'`
	`  ID(userid|groupname)`
	`  ACCESS(level)`
		"Permitting an individual or a group to use a data set" on page 80

Deny an individual or a group use of a data set	`PERMIT 'profile-name'`
	`  ID(userid|groupname) ACCESS(NONE)`
	
	or
	
	`PERMIT 'profile-name'`
	`  ID(userid|groupname) DELETE`
		"Denying an individual or a group use of a data set" on page 81

Search for general resource profile names	`SEARCH CLASS(classname)`	"Searching for general resource profile names" on page 83
List the contents of general resource profiles	`RLIST classname profile-name`	"Listing the contents of general resource profiles" on page 84

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

Task	Command	Where described

Permit an individual or a group to use a general resource	`PERMIT profile-name`
	`  CLASS(classname)`
	`  ID(userid|groupname)`
	`  ACCESS(access-authority)`
		"Permitting an individual or a group to use a general resource" on page 85

Deny an individual or a group the use of a general resource	`PERMIT profile-name CLASS(classname)`
	`  ID(userid|groupname) ACCESS(NONE)`
	or
	`PERMIT profile-name CLASS(classname)`
	`  ID(userid|groupname) DELETE`
		"Denying an individual or a group use of a general resource" on page 86

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

With the RACF remote sharing facility (RRSF), you can 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 56 for information about 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 indicating 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 that is 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 that is produced by directed commands. The format of the output is the same for both your RRSFLIST data set and for the output that is transmitted when your data set is full. Figure 2 on page 13 shows the format of output for this directed LISTGRP command:

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

Figure 3 on page 13 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 on page 14 shows the format of output for an automatically directed ADDUSER command. Figure 5 on page 14 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
```

Note:

1. RACF uses the INTERCOM setting at the time the directed command or password synchronization change occurred and if the setting was NOINTERCOM then, 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.

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 47 for information about changing your password periodically.

Log on to the system. Figure 6 on page 18 shows a sample logon panel. The sample logon panel is divided into two columns, general logon parameters and RACF logon parameters.

© Copyright IBM Corp. 1994, 2016

```
------------------------------ 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.

The sample logon panel is divided into two columns, general logon parameters and RACF logon parameters

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 contained 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 the user's 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 must 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 19 shows the fields that appear in the LISTUSER command output. “Understanding the information RACF has about you as a user” on page 19 and “Finding out what authority you have as a member of a group” on page 22 describe what this RACF information means. Figure 8 on page 25 and Figure 9 on page 26 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.

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 that is named in this field.)

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

PASS-INTERVAL
The number of days your password, or password phrase, 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 to log on successfully. The security administrator can set a system-level interval that overrides the interval that is shown for your user ID.

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

PASSWORD ENVELOPED
Indicates whether your password is *enveloped*. An enveloped password is an encrypted copy of a password that is 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 your password phrase is *enveloped*. An enveloped password phrase is an encrypted copy of a password phrase that is 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 that are 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 that is 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 94 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. For more information about password phrases, see "Changing your password phrase" on page 48.

NOPASSWORD
Indicates that you have not been assigned a password.

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, including 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.

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

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

SECURITY-LABEL
Your installation can define various security labels. A security label is a name that is 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 that are 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 want 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 19 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 that is owned by the connect group, RACF looks at UACC and allows the user to use the resource in the manner that is specified in the UACC.

The UACC can have one of the following values:

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 80 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.

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 that are 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 94 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 26.

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 52.

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 that are assigned to this operator to which BMS messages are sent (OPCLASS)
- Whether the operator is forced off when an XRFSOFF takeover occurs (XRFSOFF)
- 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
 TLSKEYS= 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 that is 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.

To see the custom field information that is 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 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 sample:

```
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 Distributed Computing Environment (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 (HOMECELL)
- The home cell's universal unique identifier (HOMEUUID)
- Whether you have single signon processing (AUTOLOGIN)

The information in the DCE segment is used by Distributed File Service (DFS) Server Message Block (SMB) support.

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
 HOMECELL= 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 sample:

```
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 sample:

```
Mapping information for user NET1ID:
 Label: General Internet 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 that is 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 that is 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= EIMDOMAINALOOKUP
```

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:

```
USER=DJONES

KERB INFORMATION
---------------
  KERBNAME= local Kerberos principle name
  MAXTKTLFE= 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
  MAXTKTLFE= 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

Note:

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)
- Type of security check (CTL)
- Whether unsolicited messages are 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 that is 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.
- 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 hardcopy (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 1-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

Note:

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.
2. 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)

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

The ASSIZEMAX value limits the combined size of above and below the 16M line storage. If ASSIZEMAX is greater than LDALIMIT (the <16M limit) then the LDAELIM (the >16M limit) is set to ASSIZEMAX - LDALIM.

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

Note:

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:

```
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

Note:

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 (except for SIZE, MAXSIZE, and USERDATA).

To see the TSO/E information that is 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” on page 43 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 50.

Finding out what user ID associations are defined for you

Your user profile might contain information about user ID associations that are 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
- 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 that are 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   Node.userid         Password  Association
  Type                             Sync      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 that are 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   Node.userid         Password  Association
  Type                             Sync      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 that are 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   Node.userid         Password  Association
  Type                             Sync      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 that are associated with your user ID, as shown in the following examples.

User NETB0Y requests the listing of its Savings Account digital certificate to ensure that it has been defined, and that it is marked trusted. The user has READ authority to the FACILITY class profile IRR.DIGTCERT.LIST. The user issues the RACDCERT command with the LIST operand, specifying the label to identify its certificate:

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

and receives the following output:

```
Digital certificate information for user NETB0Y:

 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 its key rings. The user has three key rings with certificates and one key ring that has no certificates. The user has READ

authority to the FACILITY class profile IRR.DIGTCERT.LIST. The user issues the RACDCERT command with the LISTRING operand, specifying * to list all of its 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 must 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 17.

If you have multiple user IDs, you can keep your passwords that are 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 50 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 50 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 do not know whether mixed case passwords are supported, ask your security administrator.

  If your installation supports special characters in passwords, symbolic characters other than @, #, or $, that can be used are:

  ```
  !   %   &   *   _
  +   |   :   <   >
  ?   .   -   =
  ```

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:

© Copyright IBM Corp. 1994, 2016

```
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:

```
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 19.

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 must 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 50 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 50 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 uppercase characters or sequential lowercase characters) cannot 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 quotation marks. TSO/E does not support entering quoted strings in print inhibit mode; therefore your password phrase is 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 47. 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 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 56.

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" for additional information.

Note:

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 their 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 their 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 that 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. A TSO SEND message is then received on NODE1 indicating 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 by using the TSO PROFILE command, the data set name that is 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.

Note:

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 on page 52 shows the format of output that is produced by automatic password direction. The format of the output is the same for both your RRSFLIST data set and for the output that is 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.

Note:

- In most cases the following actions are needed only if your installation does not have list-of-groups processing in effect. However, in some cases they 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 these actions are 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 perform the following actions.

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

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 18, 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 that you want to log on to in the **Group Ident** field of the logon panel. Figure 46 on page 53 shows a user logging on to group ABC123. It is also divided into two columns, General logon parameters and RACF logon parameters.

```
------------------------------ TSO/E LOGON -----------------------------

  Enter LOGON parameters below:                RACF LOGON parameters:

  Userid    ===> CLAIRE                        SECLABEL     ===>

  Password  ===> _                             New Password ===>

  Procedure ===> PROC01                        Group Ident  ===> ABC123

  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 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 are 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 that are listed are the security labels that you are authorized to use.

```
LOGOFF
```

2. Log on using a security label other than your default security label.

   Enter the security label that you want to log on with in the SECLABEL field of the logon panel. Figure 47 shows a user logging on with security label SECRET. The sample panel is divided into two columns, General logon parameters and RACF logon parameters.

```
------------------------------ TSO/E LOGON -----------------------------

  Enter LOGON parameters below:                  RACF LOGON parameters:

  Userid    ===> CLAIRE                          SECLABEL     ===> SECRET

  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 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 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.

Important: 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 restriction is because the surrogate user can do anything that 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 runs under.

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

   ```
   SEARCH CLASS(SECLABEL)
   ```

   If the security label under which the job runs 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 93 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 that 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 80.

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 no longer is 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.

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 11 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 11 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 43.

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 log on to your JDOE user ID to issue a subsequent RACLINK APPROVE command.

If you did not 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.

If a password starts with an asterisk, or if a password phrase is specified, the entire string (*target-node.target-userid/target-userid-password*) must be enclosed in single quotation marks.

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 is 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 43.

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 did not 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.

If a password starts with an asterisk, or if a password phrase is specified, the entire string (*target-node.target-userid/target-userid-password*) must be enclosed in single quotation marks.

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 43.

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 receives a notification message that this user ID association is in the process of being established. The association is pending until OPER2 issues a subsequent RACLINK APPROVE command.

If a password starts with an asterisk, or if a password phrase is specified, the entire string (*target-node.target-userid/target-userid-password*) must be enclosed in single quotation marks.

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 43.

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:

```
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 43.

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, including the data set profile, to decide whether to allow you to use it.

A data set profile contains the following information:

- 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 that are 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. Put ID(*) in the access list with the access authority you want them to have. All other users are allowed the access that you specify as the universal access authority (UACC). The access authorities that you can specify are: NONE, READ, UPDATE, CONTROL, ALTER, and EXECUTE. See “Creating a discrete profile to protect a data set” on page 61 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 61.

© Copyright IBM Corp. 1994, 2016

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 names 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 profile 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 that 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 64.

Note:

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 take any of the following actions:
   - 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 94 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 you want different protection, 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. See "Deciding which RACF protections to use."
2. Enter the ADDSD command to create the profile for the data set. See "Entering the ADDSD command to create the profile for the data set" on page 63.

Deciding 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 80.

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 have one of the following values:

  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 80 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.

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.

Entering the ADDSD command to create the profile for the data set

Use the ADDSD command to create a discrete profile for a data set.

Creating a discrete profile for a cataloged 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)
```

Creating a discrete profile for a data set that is not cataloged

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)
```

Creating a discrete profile with a NOTIFY user ID

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)
```

Creating a discrete profile for a VSAM data set

To create a discrete profile for a VSAM data set, you can use the VSAM cluster name on the ADDSD command.

For example, 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. For more information, see "Deciding how to specify the profile name."
2. Decide which RACF protections to use. For more information, see "Deciding which RACF protections to use" on page 65.
3. Enter the ADDSD command to create the profile. For more information, see "Entering the ADDSD command to create the profile" on page 67.

Deciding 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.

*** (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 90 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 92 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 91 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.

Deciding 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 use 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 80.

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 have one of the following values:

  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 80 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.

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 22.)

- 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 reuse. 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.

Entering the ADDSD command to 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 93.

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, where *prefix* is your user ID:

- If your system has enhanced generic naming:

  ```
  ADDSD 'prefix.**' UACC(NONE)
  ```
- If your system does not have enhanced generic naming:

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

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 80 or “Denying an individual or a group use of a data set” on page 81.

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 whether 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 results 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 70.

2. Determine whether 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 results 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 70.

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 61 or "Creating a generic profile to protect a data set" on page 64 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:

- 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 sample:

```
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 their 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 does not erase DASD data set extents when the data set is deleted.

Note: 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 is 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).

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 90 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 80 and "Denying an individual or a group use of a data set" on page 81.

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 68.
2. Remove RACF protection.

   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 command 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 Example 2, 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 Example 1 and Example 2, 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.

  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 61.

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*.

© Copyright IBM Corp. 1994, 2016

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 81.

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 74.

   Remember 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 have one of the following values: NONE, READ, UPDATE, CONTROL, ALTER, or EXECUTE. For descriptions of these values, see "Access authority for data sets" on page 89.

   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 80 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:

     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)
     ```

© Copyright IBM Corp. 1994, 2016

- 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 93.

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

1. Find the name of the profile that protects the data set. For more information, see “Finding out how a data set is protected” on page 68.
2. Decide whether to use the profile that protects the data set.
   - If the profile is a discrete profile, go 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 59.
3. Decide which access authority to specify for the user.

   The access authority can have one of the following values: NONE, READ, UPDATE, CONTROL, ALTER, or EXECUTE. For descriptions of these values, see “Access authority for data sets” on page 89.
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 they are RACF-defined.

Note: Neither an ID(*) entry and 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 want 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 93.

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 68.
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 59.
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 82.
   - 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 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" on page 82.

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)
```

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
  ```

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 the topic on supplied resource classes in *z/OS Security Server RACF Security Administrator's Guide*.

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, including 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 90 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.

© Copyright IBM Corp. 1994, 2016

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 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 the topic on supplied resource classes in *z/OS Security Server RACF Security Administrator's Guide*.
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)
```

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 the topic on supplied resource classes in *z/OS Security Server RACF Security Administrator's Guide*.

2. Specify the RACF profiles that 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 information is useful 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:

1. Find the name of the profile that protects the general resource. To do this, see "Searching for general resource profile names" on page 83.
2. Decide which access authority to specify in the profile. The access authority can have one of the following values: NONE, READ, UPDATE, CONTROL, and ALTER. For descriptions of these values, see "Access authority for general resources" on page 90.
3. 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:

  ```
  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 want 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 83.
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 87.
   - 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 should assign a UACC of NONE, and then selectively permit a few 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 80 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 ALTDSD 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 their 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.

© Copyright IBM Corp. 1994, 2016

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

EXECUTE
For a private load library, EXECUTE enables 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.

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 on page 93 and Table 5 on page 93 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

*Table 3. Generic naming for data sets with enhanced generic naming inactive: * in the middle or % (continued)*

Profile Name	ABC.%EF	AB.*.CD	AB.CD*.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

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 on page 93 and Table 5 on page 93 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 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 opened the data set, and you change the user's access, situations that can occur are:

- 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 events 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.

    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 on page 95 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 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

Appendix B. Accessibility

Accessible publications for this product are offered through IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSLTBW/welcome).

If you experience difficulty with the accessibility of any z/OS information, send a detailed message to the "Contact us" web page for z/OS (http://www.ibm.com/systems/z/os/zos/webqs.html) or use the following mailing address.

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Building 707
2455 South Road
Poughkeepsie, NY 12601-5400
United States

Accessibility features

Accessibility features help users who have physical disabilities such as restricted mobility or limited vision use software products successfully. The accessibility features in z/OS can help users do the following tasks:

- Run assistive technology such as screen readers and screen magnifier software.
- Operate specific or equivalent features by using the keyboard.
- Customize display attributes such as color, contrast, and font size.

Consult assistive technologies

Assistive technology products such as screen readers function with the user interfaces found in z/OS. Consult the product information for the specific assistive technology product that is used to access z/OS interfaces.

Keyboard navigation of the user interface

You can access z/OS user interfaces with TSO/E or ISPF. The following information describes how to use TSO/E and ISPF, including the use of keyboard shortcuts and function keys (PF keys). Each guide includes the default settings for the PF keys.

- *z/OS TSO/E Primer*
- *z/OS TSO/E User's Guide*
- *z/OS V2R2 ISPF User's Guide Vol I*

Dotted decimal syntax diagrams

Syntax diagrams are provided in dotted decimal format for users who access IBM Knowledge Center with a screen reader. In dotted decimal format, each syntax element is written on a separate line. If two or more syntax elements are always present together (or always absent together), they can appear on the same line because they are considered a single compound syntax element.

Each line starts with a dotted decimal number; for example, 3 or 3.1 or 3.1.1. To hear these numbers correctly, make sure that the screen reader is set to read out

© Copyright IBM Corp. 1994, 2016

punctuation. All the syntax elements that have the same dotted decimal number (for example, all the syntax elements that have the number 3.1) are mutually exclusive alternatives. If you hear the lines 3.1 USERID and 3.1 SYSTEMID, your syntax can include either USERID or SYSTEMID, but not both.

The dotted decimal numbering level denotes the level of nesting. For example, if a syntax element with dotted decimal number 3 is followed by a series of syntax elements with dotted decimal number 3.1, all the syntax elements numbered 3.1 are subordinate to the syntax element numbered 3.

Certain words and symbols are used next to the dotted decimal numbers to add information about the syntax elements. Occasionally, these words and symbols might occur at the beginning of the element itself. For ease of identification, if the word or symbol is a part of the syntax element, it is preceded by the backslash (\) character. The * symbol is placed next to a dotted decimal number to indicate that the syntax element repeats. For example, syntax element *FILE with dotted decimal number 3 is given the format 3 * FILE. Format 3* FILE indicates that syntax element FILE repeats. Format 3* * FILE indicates that syntax element * FILE repeats.

Characters such as commas, which are used to separate a string of syntax elements, are shown in the syntax just before the items they separate. These characters can appear on the same line as each item, or on a separate line with the same dotted decimal number as the relevant items. The line can also show another symbol to provide information about the syntax elements. For example, the lines 5.1*, 5.1 LASTRUN, and 5.1 DELETE mean that if you use more than one of the LASTRUN and DELETE syntax elements, the elements must be separated by a comma. If no separator is given, assume that you use a blank to separate each syntax element.

If a syntax element is preceded by the % symbol, it indicates a reference that is defined elsewhere. The string that follows the % symbol is the name of a syntax fragment rather than a literal. For example, the line 2.1 %OP1 means that you must refer to separate syntax fragment OP1.

The following symbols are used next to the dotted decimal numbers.

? indicates an optional syntax element
The question mark (?) symbol indicates an optional syntax element. A dotted decimal number followed by the question mark symbol (?) indicates that all the syntax elements with a corresponding dotted decimal number, and any subordinate syntax elements, are optional. If there is only one syntax element with a dotted decimal number, the ? symbol is displayed on the same line as the syntax element, (for example 5? NOTIFY). If there is more than one syntax element with a dotted decimal number, the ? symbol is displayed on a line by itself, followed by the syntax elements that are optional. For example, if you hear the lines 5 ?, 5 NOTIFY, and 5 UPDATE, you know that the syntax elements NOTIFY and UPDATE are optional. That is, you can choose one or none of them. The ? symbol is equivalent to a bypass line in a railroad diagram.

! indicates a default syntax element
The exclamation mark (!) symbol indicates a default syntax element. A dotted decimal number followed by the ! symbol and a syntax element indicate that the syntax element is the default option for all syntax elements that share the same dotted decimal number. Only one of the syntax elements that share the dotted decimal number can specify the ! symbol. For example, if you hear the lines 2? FILE, 2.1! (KEEP), and 2.1 (DELETE), you know that (KEEP) is the

default option for the FILE keyword. In the example, if you include the FILE keyword, but do not specify an option, the default option KEEP is applied. A default option also applies to the next higher dotted decimal number. In this example, if the FILE keyword is omitted, the default FILE(KEEP) is used. However, if you hear the lines 2? FILE, 2.1, 2.1.1! (KEEP), and 2.1.1 (DELETE), the default option KEEP applies only to the next higher dotted decimal number, 2.1 (which does not have an associated keyword), and does not apply to 2? FILE. Nothing is used if the keyword FILE is omitted.

*** indicates an optional syntax element that is repeatable**

The asterisk or glyph (*) symbol indicates a syntax element that can be repeated zero or more times. A dotted decimal number followed by the * symbol indicates that this syntax element can be used zero or more times; that is, it is optional and can be repeated. For example, if you hear the line 5.1* data area, you know that you can include one data area, more than one data area, or no data area. If you hear the lines 3* , 3 HOST, 3 STATE, you know that you can include HOST, STATE, both together, or nothing.

Notes:

1. If a dotted decimal number has an asterisk (*) next to it and there is only one item with that dotted decimal number, you can repeat that same item more than once.
2. If a dotted decimal number has an asterisk next to it and several items have that dotted decimal number, you can use more than one item from the list, but you cannot use the items more than once each. In the previous example, you can write HOST STATE, but you cannot write HOST HOST.
3. The * symbol is equivalent to a loopback line in a railroad syntax diagram.

+ indicates a syntax element that must be included

The plus (+) symbol indicates a syntax element that must be included at least once. A dotted decimal number followed by the + symbol indicates that the syntax element must be included one or more times. That is, it must be included at least once and can be repeated. For example, if you hear the line 6.1+ data area, you must include at least one data area. If you hear the lines 2+, 2 HOST, and 2 STATE, you know that you must include HOST, STATE, or both. Similar to the * symbol, the + symbol can repeat a particular item if it is the only item with that dotted decimal number. The + symbol, like the * symbol, is equivalent to a loopback line in a railroad syntax diagram.

Notices

This information was developed for products and services offered in the U.S.A. or elsewhere.

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A

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

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes 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.

© Copyright IBM Corp. 1994, 2016

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:

Site Counsel
IBM Corporation
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.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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

COPYRIGHT LICENSE:

This information might contain sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

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.

Minimum supported hardware

The minimum supported hardware for z/OS releases identified in z/OS announcements can subsequently change when service for particular servers or devices is withdrawn. Likewise, the levels of other software products supported on a particular release of z/OS are subject to the service support lifecycle of those products. Therefore, z/OS and its product publications (for example, panels, samples, messages, and product documentation) can include references to hardware and software that is no longer supported.

- For information about software support lifecycle, see: IBM Lifecycle Support for z/OS (http://www.ibm.com/software/support/systemsz/lifecycle/)
- For information about currently-supported IBM hardware, contact your IBM representative.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml (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 Oracle and/or its affiliates.

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.

Index

Special characters

A

C

D

© Copyright IBM Corp. 1994, 2016

E

F

G

H

I

K

L

M

T

U

V

W

Y

Z

Product Number: 5650-ZOS

Printed in USA

SA23-2298-02