z/VM
7.3

RACF Security Server Command Language Reference

SC24-6306-73

Note:

Before you use this information and the product it supports, read the information in "Notices" on page 351.

This edition applies to version 7, release 3 of IBM® z/VM® (product number 5741-A09) and to all subsequent releases and modifications until otherwise indicated in new editions.

Last updated: 2023-12-09

Contents

Figures

Tables

About This Document

This document describes commands supported by the IBM RACF® Security Server for z/VM.

Though this information is specific to z/VM, there are references to z/OS®. These references are applicable only when sharing a RACF database with a z/OS system, which is supported only on z/VM 7.2 and earlier versions.

Intended Audience

This document is intended for RACF-defined users who are responsible for creating, updating, or maintaining the profiles for users, groups, data sets, and general resources in the RACF database on z/OS or z/VM systems.

Readers must be familiar with the RACF concepts and terminology described in *z/VM: RACF Security Server General User's Guide*. Many RACF functions also require you to understand the more detailed descriptions in *z/VM: RACF Security Server Security Administrator's Guide*.

Where to Find More Information

For information about related publications, refer to the “Bibliography” on page 355.

Links to Other Documents and Websites

The PDF version of this document contains links to other documents and websites. A link from this document to another document works only when both documents are in the same directory or database, and a link to a website works only if you have access to the Internet. A document link is to a specific edition. If a new edition of a linked document has been published since the publication of this document, the linked document might not be the latest edition.

How to provide feedback to IBM

We welcome any feedback that you have, including comments on the clarity, accuracy, or completeness of the information. See How to send feedback to IBM for additional information.

Summary of Changes for z/VM: RACF Security Server Command Language Reference

This information includes terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations for the current edition are indicated by a vertical line (**|**) to the left of the change.

SC24-6306-73, z/VM 7.3 (December 2023)

This edition includes terminology, maintenance, and editorial changes.

SC24-6306-73, z/VM 7.3 (September 2022)

This edition supports the general availability of z/VM 7.3. Note that the publication number suffix (-73) indicates the z/VM release to which this edition applies.

SC24-6306-04, z/VM 7.2 (December 2020)

This edition includes changes to support product changes provided or announced after the general availability of z/VM 7.2.

RACF Enhancements

With the PTFs for APARs VM66459, VM66460, and VM66214, RACF has been enhanced as follows:

- The RACF command enhancements enable the RACF command processor to perform remote command execution inside an SSI cluster. This allows you to use the SETROPTS, SETEVENT, and RVARY commands the same way as they are currently supported by the RAC command. This enhancement closes the gap for automation solutions which are required to execute RACF commands while also receiving commands through SMSG (such as the DirMaint-RACF interface).
- A new SMF record exit, ICHRSWX1, is called after SMF records have been written to disk. This exit can then be used to relay SMF records to other guests. Critical SMF records can be dynamically monitored and, if necessary, specific actions can be taken.

SC24-6306-03 z/VM 7.2 (September 2020)

This edition supports the general availability of z/VM 7.2.

SC24-6306-02, z/VM 7.1 (May 2020)

This edition includes changes to support product changes provided or announced after the general availability of z/VM 7.1.

Multi-Factor Authentication for z/VM

With the PTF for APAR VM66338, Multi-Factor Authentication (MFA) provides for the establishment of a user's identity by utilizing more than one type of authentication. This provides greater security by allowing for an additional form of proof in the event that one token (for example, a password) becomes compromised. Previously, authentication of identity during the logon process could be met only by using a password or passphrase. MFA enables support for an external service to authenticate tokens that have been generated after a successful multi-factor authentication.

The following z/VM RACF commands have been updated:

- ADDUSER (Add User Profile)
- ALTUSER (Alter User Profile)
- LISTUSER (List User Profile)

SC24-6306-01, z/VM 7.1 (June 2019)

This edition includes changes to support product changes provided or announced after the general availability of z/VM 7.1.

RACF Usability Enhancements

With the PTF for APAR VM66278, RACF has been enhanced to improve the user experience and serviceability.

In "SETROPTS (Set RACF Options)" on page 288, the SETROPTS example has been updated to contain current template information.

SC24-6306-00, z/VM 7.1 (September 2018)

This edition supports the general availability of z/VM 7.1.

Chapter 1. Introduction

The profiles in the RACF database contain the information RACF needs to control access to resources. The RACF commands allow you to add, change, delete, and list the profiles for:

- Users
- Groups
- Data sets on z/OS
- General resources, which include terminals, minidisks, shared file system (SFS) directories and files, and all other resource classes defined in the RACF class descriptor table.

Most RACF functions do not require special versions or releases of the operating system or operating system components. Some, however, do require that your system be at a certain level of RACF. If you are unsure about whether or not a particular RACF function is available with your system, see your security administrator.

Refer to the “Authorization Required” section with each command for details on the authorization required.

Summary of Commands and Their Functions

RACF commands allow you to list, modify, add, and delete profiles for users, groups, connect entries, and resources. Table 1 on page 1 shows, in alphabetic order, each of the commands and its functions, and the system(s) on which you can invoke it. For a complete description of the authority required to issue a command and its operands, see *z/VM: RACF Security Server Command Language Reference*.

Table 1. Functions of RACF Commands

RACF Command	Command Functions	System
ADDDIR	• RACF-protect by a discrete or generic profile one or more SFS directories.	z/VM
ADDFILE	• RACF-protect by a discrete or generic profile one or more SFS files.	z/VM
ADDGROUP	• Define one or more new groups as a subgroup of an existing group. • On z/OS, specify a model data set profile for a group. • On z/OS, define default DFP information for a group. • On z/VM, define the OpenExtensions z/VM information for a group.	z/OS, z/VM
ADDSD [1]	• RACF-protect one or more existing data sets. • RACF-define one or more data sets brought from another system where they were RACF-protected. • RACF-define generic DATASET profiles. • Create a new data set model profile.	z/OS
ADDUSER	• Define one or more new users and connect the users to their default connect group. • Define a password, password phrase, both, or neither for one or more users. • On z/OS, specify a model data set profile for a user. • On z/OS, define CICS® operator information. • On z/OS, define default DFP information for a user. • On z/OS, define the preferred national language. • On z/OS, define default operator information. • On z/VM, define the OpenExtensions z/VM information for a user. • On z/OS, define default TSO logon information for a user. • On z/OS, define default work attributes.	z/OS, z/VM

Table 1. Functions of RACF Commands (continued)

RACF Command	Command Functions	System
ALTDIR	• Change a discrete or generic SFS directory profile.	z/VM
ALTDSD [1]	• Change one or more discrete or generic DATASET profiles. • Protect a single volume of a multivolume, non-VSAM DASD data set. • Remove protection from a single volume of a multivolume, non-VSAM DASD data set.	z/OS
ALTFILE	• Change a discrete or generic SFS file profile.	z/VM
ALTGROUP	• Change the information in one or more group profiles (such as the superior group, owner, or model profile name). • On z/OS, change or delete the default DFP information for a group. • On z/VM, add, change, or delete the information for an OpenExtensions z/VM group.	z/OS, z/VM
ALTUSER	• Change the information in one or more user profiles (such as the owner, universal access authority, or security level). • Change the password or password phrase of one or more users. • Revoke or reestablish one or more users' privileges to access the system. • Specify logging of information about the user, such as the commands the user issues. • On z/OS, change or delete CICS operator information. • On z/OS, change or delete the default DFP information for a user. • On z/OS, change the preferred national language. • On z/OS, change or delete the default operator information. • On z/VM, add, change, or delete the information for an OpenExtensions z/VM user. • On z/OS, change or delete the default TSO logon information for a user. • On z/OS, change or delete the default work attributes.	z/OS, z/VM
CONNECT	• Connect one or more users to a group. • Modify one or more users' connection to a group. • Revoke or reestablish one or more users' privileges to access the system.	z/OS, z/VM
DELDIR	• Remove RACF-protection from one or more SFS directories.	z/VM
DELFILE	• Remove RACF-protection from one or more SFS files.	z/VM
DELDSD [1]	• Delete one or more discrete or generic DATASET profiles. • Delete a discrete DATASET profile for a tape data set, while retaining the data set name in the TVTOC. • Remove a data set profile, but leave the data set RACF-indicated, when moving a RACF-protected data set to another system that has RACF.	z/OS
DELGROUP	• Delete one or more groups and their relationship to the superior group.	z/OS, z/VM
DELUSER	• Delete one or more users and remove all their connections to RACF groups.	z/OS, z/VM
END	• Terminate a RACF command session.	z/VM
HELP	• Display the function and proper syntax of RACF commands. • Display an explanation of command-related messages.	z/OS, z/VM
LDIRECT	• List the details of one or more discrete or generic DIRECTRY profiles, including the users and groups authorized to access an SFS directory.	z/VM
LFILE	• List the details of one or more discrete or generic FILE profiles, including the users and groups authorized to access the SFS file.	z/VM

Table 1. Functions of RACF Commands (continued)

RACF Command	Command Functions	System
LISTDSD [1]	• List the details of one or more discrete or generic DATASET profiles, including the users and groups authorized to access the data sets. • Determine the most specific matching generic profile for a data set.	z/OS
LISTGRP	• List the details of one or more group profiles, including the users connected to the group. • List only the information contained in a specific segment (RACF, DFP, or OVM) of the group profile.	z/OS, z/VM
LISTUSER	• List the details of one or more user profiles, including all the groups to which each user is connected. • List only the information contained in a specific segment (for example, DFP or OVM information) of a user profile.	z/OS, z/VM
PASSWORD or PHRASE	• Change your own user password or password phrase. • Change one or more users' change interval for passwords and password phrases. • Remove one or more user passwords.	z/OS, z/VM
PERMDIR	• Give or remove authority to access an SFS directory to specific users or groups. • Change the level of access authority to a directory for specific users or groups. • Copy the list of authorized users from one directory profile to another. • Delete an existing access list.	z/VM
PERMFILE	• Give or remove authority to access an SFS file to specific users or groups. • Change the level of access authority to a file for specific users or groups. • Copy the list of authorized users from one file profile to another. • Delete an existing access list.	z/VM
PERMIT	• Give or remove authority to access a resource to specific users or groups. • Change the level of access authority to a resource for specific users or groups. • Copy the list of authorized users from one resource profile to another. • Delete an existing access list.	z/OS, z/VM
RACF	• Begin a RACF command session.	z/VM
RALTER	• Change the discrete and/or generic profiles for one or more resources whose class is defined in the class descriptor table. • Maintain the global access checking tables. • Maintain security category and security level tables.	z/OS, z/VM
RDEFINE	• RACF-protect by a discrete and/or generic profile one or more resources whose class is defined in the class descriptor table. • Define the global access checking tables. • Define security category and security level tables.	z/OS, z/VM
RDELETE	• Remove RACF-protection from one or more resources whose class is defined in the class descriptor table. • Delete the global access checking tables. • Delete the security category and security level tables.	z/OS, z/VM
REMOVE	• Remove one or more users from a group and assign a new owner for any group data sets owned by the users.	z/OS, z/VM
RLIST	• List the details of discrete and/or generic profiles for one or more resources whose class is defined in the class descriptor table.	z/OS, z/VM

Table 1. Functions of RACF Commands (continued)

RACF Command	Command Functions	System
RVARY	• Dynamically deactivate and reactivate the RACF function. • Dynamically deactivate and reactivate the RACF primary and backup database. • Switch the primary and backup RACF databases. • Deactivate resource protection, for any resource whose class is defined in the class descriptor table, while RACF is deactivated.	z/OS, z/VM
SEARCH	• List the RACF profile names that meet a search criteria for a class of resources. • Create a CLIST of the RACF profile names that meet a search criteria for a class of resources.	z/OS, z/VM
SETEVENT	• Change the auditing or controlling of z/VM events. • Prevent users from issuing the DIAL, UNDIAL, and MESSAGE commands before logging on to the system. • Display the current status for z/VM events.	z/VM
SETRACF **2**	• Deactivate and reactivate RACF.	z/VM

Table 1. Functions of RACF Commands (continued)

RACF Command	Command Functions	System
SETROPTS	Dynamically set system-wide options relating to resource protection, specifically: For both z/OS and z/VM systems: • Choose the resource classes that RACF is to protect. • Gather and display RACF statistics. • Set the universal access authority (UACC) for terminals. • Specify logging of certain RACF commands and events. • Permit list-of-groups access checking. • Display options currently in effect. • Enable or disable generic profile checking on either a class-by-class or system-wide level. • Control user password syntax rules. • Establish password syntax rules. • Activate checking for previous passwords and password phrases. • Limit unsuccessful attempts to access the system using incorrect passwords and password phrases. • Control maximum change interval for passwords and password phrases. • Control mixed-case passwords. • Enable the use of special characters in passwords. • Enable the KDFAES password algorithm. • Warn of password and password phrase expiration. • Control global access checking for selected individual resources and/or generic names with selected generalized access rules. • Set the passwords for authorizing use of the RVARY command. • Initiate® refreshing of in-storage generic profile lists and global access checking tables. • Enable or disable shared generic profiles for general resources in common storage. • Enable or disable shared profiles through RACLIST processing for general resources. • Activate or deactivate auditing of access attempts to RACF-protected resources based on installation-defined security levels. • Activate enhanced generic naming. • Control whether a profile creator's user ID is automatically added to the profile's access list. For z/OS systems only: • Control the use of automatic data set protection (ADSP). • Activate profile modeling for GDG, group, and user data sets. • Activate protection for data sets with single-level names. • Control logging of real data set names. • Control the job entry subsystem (JES) options. • Activate tape data set protection. • Control whether or not data sets must be RACF-protected. • Control the erasure of scratched DASD data sets. • Activate program control.	z/OS, z/VM z/OS
SMF **3**	• Restart SMF recording. • Switch to the alternate SMF file.	z/VM
SRDIR	• List the SFS directory profile names that meet search criteria.	z/VM
SRFILE	• List the SFS file profile names that meet search criteria.	z/VM

Notes:

1. You can issue the SETRACF command only from a RACF service machine. A RACF service machine can run disconnected, thereby allowing a secondary console to issue this command.

   By default, RACF sets up the OPERATOR as the secondary console for a RACF service machine; the OPERATOR can issue the command to deactivate RACF. For example,

   ```
   SEND RACFVM SETRACF INACTIVE
   ```

   If you issue SETRACF for any RACF service machine in a multiple service machine environment, it will apply to all service machines.
2. SMF is only issued with SMSG.

Chapter 2. Basic Information for Using RACF Commands

You can use the RACF commands to add, modify, or delete RACF profiles and to define system-wide options. Before you can issue a RACF command, you must be defined to RACF with a sufficient level of authority. In addition, to issue the RACF commands from the foreground, you must be defined to the system.

How to Enter RACF Commands

The following sections describe how to enter RACF commands. You can enter RACF commands by preceding the command name with RAC, or by entering a RACF command session. You must be authorized to enter a RACF command session.

You can also enter RACF commands by using the RACF ISPF panels.

Choosing between Using RACF Commands and ISPF Panels

In general, you can perform the same RACF functions using RACF commands and ISPF panels.

The **RACF commands** provide the following advantages:

- Entering commands can be faster than displaying many panels in sequence.
- Using commands from book descriptions should be relatively straightforward. The examples in the books are generally command examples.
- Getting online HELP
  - To see online help for the PERMIT command when you are using the RAC command, enter:

    ```
    RAC HELP PERMIT
    ```

  - In a RACF command session, enter:

    ```
    HELP PERMIT
    ```

  - To limit the information displayed, specify operands on the HELP command. To see only the syntax of the PERMIT command, enter:

    ```
    HELP PERMIT SYNTAX
    ```

    or

    ```
    RAC HELP PERMIT SYNTAX
    ```

- If you use the RAC command processor on VM, the RACF command output is displayed on the screen and also written to the RACF DATA file on the user's specified disk or directory (file mode A is the default).

The *ISPF panels* provide the following advantages:

- ISPF creates a summary record in the ISPF log of the work that you do; unless you spool your console on z/VM (see *z/VM: CMS User's Guide*), the RACF commands do not create such a record.
- From the panels, you can press the HELP key to display brief descriptions of the fields on the panels.
- The options chosen when installing the RACF panels determine whether output (for example, profile listings, search results, RACF options, and VM event settings) is displayed in a scrollable form.

  On VM, if your installation uses XEDIT for display in ISPF, you can even save the listings on your disk or directory accessed as A. You can also save the output from a SEARCH in a REXX exec.

- The ISPF panels for working with VM events provide selection lists. Using the selection lists, you can avoid typing errors when specifying RACF event names.
- The ISPF panels for working with password rules allow you to enter all the password rules on one panel.

Entering RACF Commands

Using RAC

You can enter RACF commands during a z/VM terminal session by entering

```
RAC    any-RACF-command
```

This enables you to enter RACF commands without isolating yourself in a RACF command session. You can continue entering CP or CMS commands.

If you need to enter a command that is longer than the z/VM command line allows, you may choose one of the following methods.

- You may write an exec similar to the one following:

```
/* */
trace "o"
cmd = "adduser ewing data('This is a sample of a large amount"
cmd = cmd||" of installation data that exceeds the command line"
cmd = cmd||" limit of one hundred thirty characters of any"
cmd = cmd||" information that the user would like to enter')"
rac cmd
```

- To enter the command interactively, issue the RAC command with no operands. The RAC exec will prompt you to enter command data. Keep entering lines of the RACF command until you are finished. Next, enter a null line. The RAC command processor will send the complete command to the RACF service machine for processing.

  When you enter a RACF command using the above method, the RAC exec accepts your input exactly as is. Remember to enter spaces at the end of a given line of input if necessary.

Up to 3500 characters will be accepted by the RAC command processor. If this limit is exceeded, you will receive an error message.

See *z/VM: RACF Security Server System Programmer's Guide* and the description of “RAC (Enter RACF Commands on z/VM)” on page 207 for more information.

Using the RACF Command Session

If permitted, you can enter RACF commands by entering a RACF command session. Issue the following command:

```
RACF
```

Note:

1. RACF does not require you to enter a password or password phrase to establish a RACF command session. Your installation, however, may require it. If your installation requires a password or password phrase, RACF prompts you for your logon password or password phrase. You can change your password or password phrase when the password or password phrase prompt appears; if you are then denied access because your installation has restricted usage of RACF, your password or password phrase change is still in effect. After you have entered your password or password phrase, you can issue the RACF commands for which you have sufficient authority.
2. When you are in a RACF command session , you can issue **only** valid RACF commands. CMS commands are not valid in a RACF environment, even though they are valid on your z/VM system.

The command examples in this book use uppercase letters; however, when you are entering commands from a terminal, you can use either uppercase or lowercase letters.

To terminate a RACF session at any time, issue the following command:

```
END
```

IKJ Messages:

If you make a mistake entering a RACF command in a RACF command session, IKJ messages such as `INVALID KEYWORD` and `REENTER THIS OPERAND` appear. They describe the syntax error found and prompt you to reenter the input. To escape from this prompt:

1. Type `hx` and press Enter.
2. When you get a READY prompt, type `hx` and press Enter again.

At this point, you can continue the RACF command session, or type `END` and press Enter to exit the RACF command session.

Using RACFISPF

Attention

RACFISPF will not be enhanced in the future. Its function remains at the RACF 1.9.0 level. General users should use the RAC command instead of RACFISPF to enter RACF commands. Installation applications that use RACFISPF should be updated to use the RAC EXEC instead.

You can enter RACF commands during a z/VM terminal session by invoking the RACFISPF module. RACFISPF establishes an environment in which both RACF commands and CMS commands can be issued.

RACFISPF Restricted Usage Note

RACFISPF may have restricted usage. It is recommended that general users enter RACF commands with the RAC command. Customer applications that use RACFISPF should be migrated to the RAC EXEC. If you need to use RACFISPF and are not authorized, contact your security administrator.

To establish a RACFISPF environment, type `RACFISPF` and press Enter.

Using RACFISPF, output from RACF commands can be saved in one of two files: RACF DATA or R$CLIST EXEC. R$CLIST EXEC is intended to be used for the output of the SEARCH command with the CLIST option. RACF DATA is merely a listing of the RACF command output.

The following options can be specified in order to save RACF output:

(DISK
: The DISK operand specifies that the output of all RACF commands while in this session will be written to the RACF DATA file on your A-disk. Each time a new command generates output, the contents of RACF DATA will be overwritten. RACF DATA will be erased when the session ends.

(APPEND
: The APPEND operand specifies that the output of all RACF commands while in this session will be written to the RACF DATA file on your A-disk. If RACF DATA already exists, command output from this session will be added to the end of the existing file. RACF DATA will be saved when the session ends.

  Note: The CLIST operand applies only to SEARCH command output and must follow either the DISK or APPEND operands.

(DISK CLIST
: The CLIST operand used with the DISK operand specifies that output from the SEARCH command with the CLIST option will be written to the R$CLIST EXEC file on your A-disk. Each time a new SEARCH command generates output, the contents of R$CLIST EXEC is overwritten. Output from all other RACF commands will be written to the RACF DATA file on your A-disk. Each time a new command generates output, the contents of RACF DATA will be overwritten. When the session ends, the R$CLIST EXEC will be saved, and RACF DATA will be erased.

(APPEND CLIST
The CLIST operand used with the APPEND operand specifies that output from the SEARCH command with the CLIST option will be written to the R$CLIST EXEC file on your A-disk. If the R$CLIST EXEC already exists, SEARCH command output will be added to the end of the existing file. Output from all other RACF commands will be written to the RACF DATA file on your A-disk. If RACF DATA already exists, command output from this session will be added to the end of the existing file. When the session ends, both the R$CLIST EXEC and RACF DATA will be saved.

To exit the RACFISPF environment at any time, type END and press Enter.

Note:

1. RACF does not require you to enter a password or password phrase to establish a RACFISPF environment. Your installation, however, may require it. If your installation requires a password or password phrase, RACFISPF prompts you for your logon password or password phrase. You can change your password or password phrase when the prompt appears; if you are then denied access because your installation has restricted usage of RACFISPF, your password or password phrase change is still in effect.

   If you have entered your password or password phrase and are authorized to use RACFISPF, you can then enter valid RACF z/VM commands.
2. When using RACFISPF, you should be aware that it is possible for RACF commands to produce a large amount of output. Therefore, you should be sure there is sufficient space on your A-disk.

Syntax of RACF Commands and Operands

When entering commands, one or more blanks or a comma are valid delimiters for use between operands.

The syntax for all occurrences of the *userid*, *group-name*, *password*, *class-name*, *profile-name*, *volume-serial*, and *terminal-name* operands in this book is as follows:

userid
One to eight characters, which may consist of any combination of A-Z, 0-9, # (X'7B'), $ (X'5B'), or @ (X'7C').

For z/OS users who are defined to RACF, the user ID cannot exceed seven characters and must begin with an alphabetic, # (X'7B'), $ (X'5B'), or @ (X'7C') character.

group–name
One to eight alphanumeric characters beginning with an alphabetic, # (X'7B'), $ (X'5B'), or @ (X'7C') character.

password
One to eight alphanumeric characters. Special characters are allowed if SETR PASSWORD(SPECIALCHARS) is in effect. Each installation can define its own password syntax rules. Lowercase alphanumeric characters are valid and maintained in the case entered if SETR PASSWORD(MIXEDCASE) is in effect.

password phrase
14-100 (9-100 if allowed by ICHPWX11) alphabetic and non-alphabetic (numeric, punctuation, special) characters, enclosed in single quotation marks. See “PASSWORD or PHRASE (Specify User Password or Password Phrase)” on page 190 for full password phrase syntax rules.

class–name
Valid class names are USER, GROUP, DATASET, and those classes defined in the class descriptor table (CDT).

The IBM-supplied entries in the class descriptor table are listed in Appendix B, “IBM-Supplied Resource Classes that Apply to z/VM Systems,” on page 349.

profile-name
Either a discrete name or a generic name, as described in Appendix A, “Resource Profile Naming Considerations,” on page 335.

Return Codes from RACF Commands

All of the RACF commands (except RVARY) issue the following return codes. RVARY issues return codes of 0, 8, and 12.

Decimal Code
Meaning

0
Normal completion.

4
The command encountered an error and attempted to continue processing.

8
The command encountered a user error or an authorization failure and terminated processing.

12
The command encountered a system error and terminated processing.

You can use REXX exec processing to interrogate the return codes.

RACF Command Session Return Codes

For an explanation of the RACF command session return codes, see *z/VM: RACF Security Server Messages and Codes*.

Installation Exit Routines from RACF Commands

RACF provides exits that can be used by installation-written routines when certain RACF commands are issued. The commands that have installation exits are:

ADDDIR	**ALTFILE**	**DELGROUP**	**PASSWORD**	**RALTER**	**RLIST**
ADDFILE	**ALTUSER**	**DELUSER**	**PERMDIR**	**RDEFINE**	**SEARCH**
ADDSD	**DELDIR**	**LDIRECT**	**PERMFILE**	**RDELETE**	**SRDIR**
ALTDIR	**DELDSD**	**LFILE**	**PERMIT**	**REMOVE**	**SRFILE**
ALTDSD	**DELFILE**	**LISTDSD**	**RAC**		

Your location might use installation-written exit routines to take additional security actions during the processing of the RACF commands, and these actions can affect the results you get when you issue a RACF command. For example, your location could use the ICHPWX01 preprocessing exit to install its own routine to examine a new password and new password interval.

For a complete description of these exits, see *z/VM: RACF Security Server System Programmer's Guide*.

Attribute and Authority Summary

Each command description in this book includes a section called “RACF Requirements,” which describes how attributes and authorities affect your use of that command.

Group Authorities

The group authorities, which define user responsibilities within the group, are shown below in order of least to most authority. Each level includes the privileges of the levels above it.

USE
Allows the user to access resources to which the group is authorized

CREATE
Allows the user to create RACF data set profiles for the group

CONNECT
Allows the user to connect other users to the group

JOIN
Allows the user to add new subgroups or users to the group, as well as assign group authorities to the new members

For more information on group authority, refer to *z/VM: RACF Security Server Security Administrator's Guide*.

Access Authority for SFS Files and Directories on z/VM

Shared file system (SFS) files and directories on z/VM can have one of the following access authorities:

NONE
The user or group is denied access to the SFS directory or file.

Attention:
Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected SFS file or directory can create copies of the data in them. If a user copies the data files to an SFS file or directory for which they can control the security characteristics, they can downgrade the security characteristics of the copied files. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your SFS file or directory, as their needs become known. See *z/VM: RACF Security Server General User's Guide* for information on how to permit selected users or groups to access an SFS file or directory.

READ
The user or group is authorized to access the SFS directory or file for reading only.

UPDATE
The user or group is authorized to access the SFS directory or file for reading or writing. However, UPDATE does not authorize a user to erase, discard, rename, or relocate the SFS file or directory.

CONTROL
Equivalent to UPDATE.

ALTER
Allows users to read, update, erase, discard, rename, or relocate the SFS file or directory.

- 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 DIRECTRY profile, ALTER allows users to create SFS directories protected by the profile.
- When specified in a generic FILE profile, ALTER allows users to create SFS files protected by the profile.

Note: The actual access authorities required for specific SFS operations depends on the operation itself. Multiple authorities might be required. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

Access Authority for Minidisks on z/VM

Minidisks on z/VM can have one of the following access authorities:

NONE
Does not allow users to access the minidisk.

Attention
Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected minidisk can copy the data in it. If users copy the data to a minidisk for which they can control the security characteristics, they can potentially downgrade the security characteristics of the copied files. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your minidisk, as their needs become known. See *z/VM: RACF Security Server General User's Guide* for information on how to permit selected users or groups to access a minidisk.

READ
Allows users to read from the minidisk. This enables users to request any read-only link mode on the CP LINK command. Read-only link modes include R, RR, SR, and ER. (Note that users who can read files on a minidisk can copy or print them.)

UPDATE
Allows users to read from, or write to, the minidisk. This enables users to request any of the read-only and some of the write link modes on the CP LINK command. The allowed write link modes include W, WR, SW, and EW.

CONTROL
Allows users to read from, or write to, the minidisk. This enables users to request any of the read-only link modes and all of the write link modes except MW on the CP LINK command. In addition to the link modes allowed for READ and UPDATE access, users may request a link mode of M, MR, or SM.

ALTER
Allows users to read from, or write to, the minidisk. This enables users to request any valid link mode on the CP LINK command, including MW (multiwrite).

Unlike other general resource classes, ALTER access to a discrete VMMDISK profile does not, by itself, allow a user to read, alter, or delete the profile, or to modify its access list.

As an alternative approach to allow users to manage VMMDISK profiles, you can create a group to own the profiles and connect users to that group with the SPECIAL attribute. For example, to enable users USERA and USERB to manage VMMDISK profiles for USER1.191, use the following RACF commands:

```
ADDGROUP ADMVMMD
RALTER VMMDISK USER1.191 OWNER(ADMVMMD)
CONNECT (USERA USERB) GROUP(ADMVMMD) SPECIAL
```

Users with ALTER access to a generic VMMDISK profile have no authority over the profile itself.

Note: For a description of the different CP LINK access modes, refer to *z/VM: CP Commands and Utilities Reference*.

Chapter 3. The RACF Commands

This chapter gives the syntax and function for each RACF command. The commands are presented in alphabetical order.

The description for each command starts on a right-hand page; thus, you can separate the descriptions to provide a tailored package for the users of your system based on their needs and authorities to issue the commands.

Each command description identifies which system or systems (z/OS, z/VM, or both) the command applies to. In addition, each command description contains several examples. Each example also identifies the applicable system or systems.

Although parse routines can allow the abbreviation of operands to the least number of characters that uniquely identify the operand, it is a good practice to fully spell out all operands on commands that are hard-coded (as in programs and EXECs, for example) to avoid conflicts.

Note: RACF database sharing with z/OS is not supported on z/VM 7.3 and later versions. The RACF commands and operands for z/OS are tolerated for upward compatibility but have no effect on a database that is not shared with z/OS.

1. UPPERCASE LETTERS or WORDS must be coded as they appear in the syntax diagrams, but do not have to be uppercase.
2. Lowercase letters or words represent variables for which you must supply a value.
3. Parentheses () must be entered exactly as they appear in the syntax diagram.
4. An ellipsis ... (three consecutive periods) indicates that you can enter the preceding item more than once.
5. A single item in brackets [ ] indicates that the enclosed item is optional. Do not specify the brackets in your command.
6. Stacked items in brackets [ ] indicate that the enclosed items are optional. You can choose one or none. Do not specify the brackets in your command.
7. Stacked items in braces { } indicate that the enclosed items are alternatives. You must specify one of the items. Do not specify the braces in your command.

   Note: When you select a bracket that contains braces, you must specify one of the alternatives enclosed within the braces.
8. An underlined operand indicates the default value when no alternate value is specified.
9. **BOLDFACE** or **boldface** indicates information that must be given for a command.
10. single quotation marks ' ' indicate that information must be enclosed in single quotation marks.

Figure 1. Key to Symbols in Command Syntax Diagrams

ADDDIR (Add SFS Directory Profile)

System environment

SFS directories apply to z/VM systems only.

Purpose

Use the ADDDIR command to RACF-protect an SFS directory with either a discrete or generic profile. The ADDDIR command adds a profile for the resource to the RACF database in order to control access to the SFS directory. It also places your user ID on the access list and gives you ALTER authority to the SFS directory.

Related Commands

- To change an SFS directory profile, use the ALTDIR command as described in "ALTDIR (Alter SFS Directory Profile)" on page 66.
- To delete an SFS directory profile, use the DELDIR command as described in "DELDIR (Delete SFS Directory Profile)" on page 134.
- To list the information in the SFS directory profiles, use the LDIRECT command as described in "LDIRECT (List SFS Directory Profile)" on page 148.
- To permit or deny access to an SFS directory profile, use the PERMDIR command as described in "PERMDIR (Maintain SFS Directory Access Lists)" on page 194.
- To obtain a list of SFS directory profiles, use the SRDIR command as described in "SRDIR (Obtain a List of SFS Directory Profiles)" on page 324

Authorization Required

To protect an SFS directory with RACF, one or more of the following must be true:

- The user ID qualifier of the directory profile name must match your user ID.
- You must have the SPECIAL attribute.
- The user ID (second qualifier) for the directory profile must be within the scope of a group in which you have the group-SPECIAL attribute.
- To assign a security category to a profile, you must have the SPECIAL attribute or have the category in your user profile.
- To assign a security level to a profile, you must have the SPECIAL attribute or, in your own profile, a security level that is equal to or greater than the security level you are defining.
- To assign a security label, you must have the SPECIAL attribute or have READ access to the SECLABEL profile. However, the security administrator can limit the ability to assign security labels to only users with the SPECIAL attribute.
- If the SETROPTS GENERICOWNER option is in effect, and if a generic profile already exists, *more specific* profiles that protect the same resources can be created only by the following users:
  - The owner of the existing generic profile
  - A user with system-SPECIAL
  - A user with group-SPECIAL if the group owns the profile
  - A user with group-SPECIAL if the owner of the existing profile is in the group

To protect a directory for someone else, you need to have the SPECIAL attribute or the directory profile is within the scope of a group in which you have the group-SPECIAL attribute.

Note: You do not need the SPECIAL attribute to specify the OWNER operand.

Model Profiles

To specify a model profile (using, as required, FROM, FCLASS, and FGENERIC), you must have sufficient authority over the model profile —the "from" profile. RACF makes the following checks until one of these conditions is met:

- You have the SPECIAL attribute.
- The "from" profile is within the scope of a group in which you have the group-SPECIAL attribute.
- You are the owner of the "from" profile.
- If the FCLASS operand is FILE or DIRECTRY, or defaults to DIRECTRY, the user ID qualifier of the profile name is your user ID.
- If the FCLASS operand is DATASET, the high-level qualifier of the profile name (or the qualifier supplied by the naming conventions routine or a command installation exit) is your user ID.

For discrete profiles only:

- You are on the access list in the "from" profile with ALTER authority. (If you have any lower level of authority, you cannot use the profile as a model.)
- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is on the access list in the "from" profile with ALTER authority. (If any group that RACF checked has any lower level of authority, you cannot use the profile as a model.)
- The universal access authority (UACC) is ALTER.

Syntax

The complete syntax of the ADDDIR command is:

```
ADDDIR              profile-name
ADIR                [ ADDCATEGORY(category-name ...) ]
                    [ APPLDATA('application-defined-data') ]
                    [ AUDIT( access-attempt [(audit-access-level)] ...) ]
                    [ DATA('installation-defined-data') ]
                    [ FCLASS(profile-name-2-class) ]
                    [ FGENERIC ]
                    [ FROM(profile-name-2) ]
                    [ LEVEL(nn) ]
                    [ NOTIFY [(userid)] ]
                    [ OWNER(userid or group-name) ]
                    [ SECLABEL(security-label) ]
                    [ SECLEVEL(security-level) ]
                    [ UACC(access-authority) ]
                    [ WARNING ]
```

Note: This command is an extension of the RDEFINE command as it applies to the DIRECTRY class. Other RDEFINE parameters, such as SESSION and TIMEZONE are also accepted on the command, but are not listed here. If they are specified on this command, they will be ignored.

Parameters

profile-name
specifies the name of the discrete or generic profile to be added to the RACF database. You may specify only one profile.

For more information, see "Names for SFS Directories" on page 346.

This operand is required and must be the first operand following ADDDIR.

Note: Do not specify a generic character unless SETROPTS GENERIC (or SETROPTS GENCMD) is in effect.

ADDCATEGORY(*category-name ...*)
specifies one or more names of installation-defined security categories. The name(s) you specify must be defined as members of the CATEGORY profile in SECDATA class. (For information on defining security categories, see *z/VM: RACF Security Server Security Administrator's Guide*.)

When SECDATA class is active and you specify ADDCATEGORY, RACF performs security category checking in addition to its other authorization checking. If a user requests access to a directory, RACF compares the list of security categories in the user's profile with the list of security categories in the directory profile. If RACF finds any security category in the directory profile that is not in the user's profile, RACF denies access to the directory. If the user's profile contains all the required security categories, RACF continues with other authorization checking.

When the SECDATA class is not active, RACF ignores this operand. When the CATEGORY profile does not include a member for a category-name, you are prompted to provide a valid category-name.

APPLDATA('*application-defined-data*')
specifies a text string that will be associated with the named resource. The text string may contain a maximum of 255 characters and must be enclosed in single quotation marks. It may also contain double-byte character set (DBCS) data.

AUDIT(*access-attempt* [(*audit-access-level*)])

(*access-attempt*)
specifies which access attempts you want logged on the SMF data file. The following options are available:

ALL
indicates that you want to log both authorized accesses and detected unauthorized access attempts.

FAILURES
indicates that you want to log detected unauthorized attempts.

NONE
indicates that you do not want any logging to be done.

SUCCESS
indicates that you want to log authorized accesses.

(*audit-access-level*)
specifies which access level(s) you want logged on the SMF data file. The levels you can specify are:

ALTER
logs ALTER access-level attempts only.

CONTROL
logs access attempts at the CONTROL and ALTER levels.

READ
logs access attempts at any level. READ is the default value if you omit *audit-access-level*.

UPDATE
logs access attempts at the UPDATE, CONTROL, and ALTER levels.

FAILURES(READ) is the default value if you omit the AUDIT operand.

DATA('*installation-defined-data*')
specifies up to 255 characters of installation-defined data to be stored in the directory profile. The data must be enclosed in single quotation marks. It may also contain double-byte character set (DBCS) data.

Use the LDIRECT command to list this information.

FCLASS(*profile-name-2-class*)
specifies the name of the class to which *profile-name-2* belongs. The valid class names are DIRECTRY, FILE, DATASET, or other classes defined in the class descriptor table. For a list of general resource classes applied by IBM, see Appendix B, "IBM-Supplied Resource Classes that Apply to z/VM Systems," on page 349. If you omit this operand, RACF assumes the DIRECTRY class. This operand is valid only when you also specify the FROM operand; otherwise, RACF ignores it.

FGENERIC
specifies that RACF is to treat *profile-name-2* as a generic name, even if it does not contain any generic characters. This operand is needed only if *profile-name-2* is a DATASET profile.

FROM(*profile-name-2*)
specifies the name of an existing discrete or generic profile that RACF is to use as a model for the new profile. The model profile name you specify on the FROM operand overrides any model name specified in your user or group profile. If you specify FROM and omit FCLASS, RACF assumes that *profile-name-2* is the name of a profile in the DIRECTRY class.

If FCLASS is not specified or FCLASS(DIRECTRY) is specified, *profile-name-2* must be the name of a profile in the DIRECTRY class. If FCLASS(FILE) is specified, *profile-name-2* must be the name of a profile in the FILE class. For the formats of these profile names, see "Profile Names for SFS Files and Directories" on page 342.

To specify FROM, you must have sufficient authority to both the *profile-name and profile-name-2*, as described in "Authorization Required" on page 16.

Possible Changes to Copied Profiles When Modeling Occurs

When a profile is copied during profile modeling, the new profile could differ from the model in the following ways:

- RACF either places the user on the access list with ALTER access authority or, if the user is already on the access list, RACF changes the user's access authority to ALTER.
- If the SETROPTS MLS option is in effect, the security label, if specified in the model profile, is not copied. Instead, the user's current security label is used.

  EXCEPTION: When SETROPTS MLS and MLSTABLE are both in effect and the user has the SPECIAL attribute, the security label specified in the model profile is copied to the new profile.

For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

LEVEL(*nn*)
specifies a level indicator, where *nn* is an integer between 0 and 99. The default is 0.

Your installation assigns the meaning of the value.

RACF includes it in all records that log SFS directory accesses and in the LDIRECT command display.

NOTIFY[(*userid*)]
specifies the user ID of a user to be notified whenever RACF uses this profile to deny access to a directory. If you specify NOTIFY without specifying a user ID, RACF takes your user ID as the default; you will be notified whenever the profile denies access to a directory.

A user who is to receive NOTIFY messages should log on frequently to take action in response to the unauthorized access attempt described in each message. RACF sends NOTIFY messages as follows to the specified user ID. If the user ID is logged on, the message immediately appears on the user's screen. If the user ID is not logged on or is disconnected, RACF sends the message to the user in a reader file. The name of this reader file will be the user ID specified on the NOTIFY keyword, and the type will be NOTIFY. (Note that you should not specify the user ID of a virtual machine that always runs disconnected.)

When the directory profile also includes WARNING, RACF might have granted access to the directory to the user identified in the message.

OWNER(*userid* or *group-name*)
specifies a RACF-defined user or group to be assigned as the owner of the directory profile.

If you omit this operand, you are defined as the owner of the directory profile.

If you specify OWNER(userid), the user you specify as the owner does not automatically have access to the directory. Use the PERMDIR command to add the owner to the access list as desired.

SECLABEL(*security-label*)
specifies an installation-defined security label for this profile. A security label corresponds to a particular security level (such as CONFIDENTIAL) with a set of zero or more security categories (such as PAYROLL or PERSONNEL).

For a list of security labels that you are authorized to use, enter:

```
SEARCH CLASS(SECLABEL)
```

RACF stores the name of the security label you specify in the directory profile if you are authorized to use *security-label*.

If you are not authorized to the SECLABEL or if the name you had specified is not defined as a SECLABEL profile in the SECLABEL class, the directory profile is not created.

Note: If the SECLABEL class is active and the security label is specified in this profile, any security levels and categories in the profile are ignored.

SECLEVEL(*security-level*)
specifies the name of an installation-defined security level. This name corresponds to the number that is the minimum security level that a user must have to access the directory. The *security-level* must be a member of the SECLEVEL profile in the SECDATA class.

When you specify SECLEVEL and the SECDATA class is active, RACF adds security level access checking to its other authorization checking. If global access checking does not grant access, RACF compares the security level allowed in the user profile with the security level required in the directory profile. If the security level in the user profile is less than the security level in the directory profile, RACF denies the access. If the security level in the user profile is equal to or greater than the security level in the directory profile, RACF continues with other authorization checking.

If the SECDATA class is not active, RACF stores the name you specify in the directory profile. When the SECDATA class is activated and the name you specified is defined as a SECLEVEL profile, RACF can perform security level access checking for the directory profile. If the name you specify is not defined as a SECLEVEL profile and the SECDATA class is active, you are prompted to provide a valid *security-level*.

UACC(*access-authority*)
specifies the universal access authority to be associated with the directory. The universal access authorities are ALTER, CONTROL, UPDATE, READ, and NONE. For more information, see “Access Authority for SFS Files and Directories on z/VM” on page 12.

If UACC is not specified, RACF uses the value in the ACEE or the class descriptor table. If UACC is specified without an access-authority, RACF uses the value in the current connect group.

WARNING
specifies that, even if access authority is insufficient, RACF is to issue a warning message and allow access to the directory. RACF also records the access attempt in the SMF record if logging is specified in the profile.

Examples

Example 1

Operation: User SMITH wants to create a discrete profile to protect his directory (DIR1) in file pool POOL1.

Known: User SMITH is RACF-defined and owns directory DIR1.

Command:
```
ADDDIR POOL1:SMITH.DIR1 UACC(NONE)
```

Defaults: OWNER(SMITH), AUDIT(FAILURES(READ)), LEVEL(0)

Example 2

Operation: User SMITH wants to create a generic profile to protect his directory (DIR1) in file pool POOL1 and all of its subdirectories. His directory is classified SECRET.

Known: User SMITH is RACF-defined, owns directory DIR1, and is authorized to security label, SECRET.

Command:
```
ADDDIR POOL1:SMITH.DIR1.** SECLABEL(SECRET)
UACC(NONE)
```

Defaults: OWNER(SMITH), AUDIT(FAILURES(READ)), LEVEL(0)

ADDFILE (Add SFS File Profile)

System environment

SFS files apply to z/VM systems only.

Purpose

Use the ADDFILE command to RACF-protect SFS files with either discrete or generic profiles. The ADDFILE command adds a profile for the resource to the RACF database in order to control access to the SFS file. It also places your user ID on the access list and gives you ALTER authority to the SFS file.

Related Commands

- To change an SFS file, use the ALTFILE command as described in "ALTFILE (Alter SFS File Profile)" on page 81.
- To delete an SFS file profile, use the DELFILE command as described in "DELFILE (Delete SFS File Profile)" on page 139.
- To list the information in the SFS file profiles, use the LFILE command as described in "LFILE (List SFS File Profile)" on page 154.
- To permit or deny access to an SFS file, use the PERMFILE command as described in "PERMFILE (Maintain SFS File Access Lists)" on page 198.
- To obtain a list of SFS file profiles, use the SRFILE command as described in "SRFILE (Obtain a List of SFS File Profiles)" on page 329.

Authorization Required

To protect an SFS file with RACF, one or more of the following must be true:

- The user ID qualifier of the file name must match your user ID.
- You must have the SPECIAL attribute.
- The user ID qualifier for the file profile must be within the scope of a group in which you have the group-SPECIAL attribute.
- To assign a security category to a profile, you must have the SPECIAL attribute or have the category in your user profile.
- To assign a security level to a profile, you must have the SPECIAL attribute or, in your own profile, a security level that is equal to or greater than the security level you are defining.
- To assign a security label, you must have the SPECIAL attribute or have READ access to the SECLABEL profile. However, the security administrator can limit the ability to assign security labels to only users with the SPECIAL attribute.
- If the SETROPTS GENERICOWNER option is in effect, and if a generic profile already exists, *more specific* profiles that protect the same resources can be created only by the following users:
  - The owner of the existing generic profile
  - A user with system-SPECIAL
  - A user with group-SPECIAL if the group owns the profile
  - A user with group-SPECIAL if the owner of the existing profile is in the group

You cannot protect a file for someone else (the user ID qualifier is not your user ID) unless you have the SPECIAL attribute or the file profile is within the scope of a group in which you have the group-SPECIAL attribute.

Note: You do not need the SPECIAL attribute to specify the OWNER operand.

Model Profiles

To specify a model profile (using, as required, FROM, FCLASS and FGENERIC), you must have sufficient authority over the model profile — the "from" profile. RACF makes the following checks until one of the conditions is met:

- You have the SPECIAL attribute.
- The "from" profile is within the scope of a group in which you have the group-SPECIAL attribute.
- You are the owner of the "from" profile.
- If the FCLASS operand is FILE or DIRECTRY or defaults to FILE, the user ID qualifier of the profile name is your user ID.
- If the FCLASS operand is DATASET, the high-level qualifier of the profile name (or the qualifier supplied by the naming conventions routine or a command installation exit) is your user ID.

For discrete profiles only:

- You are on the access list in the "from" profile with ALTER authority. (If you have any lower level of authority, you cannot use the profile as a model.)
- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is on the access list in the "from" profile with ALTER authority. (If any group that RACF checked has any lower level of authority, you cannot use the profile as a model.)
- The universal access authority (UACC) is ALTER.

Syntax

The complete syntax of the ADDFILE command is as follows:

```
ADDFILE             profile-name
AF                  [ ADDCATEGORY(category-name ...) ]
                    [ APPLDATA('application-defined-data') ]
                    [ AUDIT( access-attempt [(audit-access-level)] ...)]
                    [ DATA('installation-defined-data') ]
                    [ FCLASS(profile-name-2-class) ]
                    [ FGENERIC ]
                    [ FROM(profile-name-2) ]
                    [ LEVEL(nn) ]
                    [ NOTIFY [(userid) ] ]
                    [ OWNER(userid or group-name) ]
                    [ SECLABEL(security-label) ]
                    [ SECLEVEL(security-level) ]
                    [ UACC(access-authority) ]
                    [ WARNING ]
```

Note: This command is an extension of the RDEFINE command as it applies to the FILE class. Other RDEFINE parameters, such as SESSION and TIMEZONE are also accepted on the command, but are not listed here. If they are specified on this command, they will be ignored.

Parameters

profile-name
specifies the name of the discrete or generic profile to be added to the RACF database. You may specify only one profile. For more information, see "Generic Characters in SFS Names" on page 345.

This operand is required and must be the first operand following ADDFILE.

Note: Do not specify a generic character unless SETROPTS GENERIC (or SETROPTS GENCMD) is in effect.

ADDCATEGORY(*category-name ...*)
specifies one or more names of installation-defined security categories. The *category-name* you specify must be defined as a member of the CATEGORY profile in the SECDATA class. (For information on defining security categories, see *z/VM: RACF Security Server Security Administrator's Guide*.)

When the SECDATA class is active and you specify ADDCATEGORY, RACF performs security category checking in addition to its other authorization checking. If a user requests access to a file, RACF compares the list of security categories in the user's profile with the list of security categories in the file profile. If RACF finds any security category in the file profile that is not in the user's profile, RACF denies access to the file. If the user's profile contains all the required security categories, RACF continues with other authorization checking.

When the SECDATA class is not active, RACF ignores this operand. When the CATEGORY profile does not include a member for a category-name, you are prompted to provide a valid category-name.

APPLDATA('*application-defined-data*')
specifies a text string that will be associated with the named resource. The text string may contain a maximum of 255 characters and must be enclosed in single quotation marks. It may also contain double-byte character set (DBCS) data.

AUDIT(*access-attempt* [(*audit-access-level*)])

(*access-attempt*)
specifies which access attempts you want logged on the SMF data file The following options are available:

ALL | FAILURES | NONE | SUCCESS

ALL
indicates that you want to log both authorized accesses and detected unauthorized access attempts.

FAILURES
indicates that you want to log detected unauthorized attempts.

NONE
indicates that you do not want any logging to be done.

SUCCESS
indicates that you want to log authorized accesses.

(*audit-access-level*)
specifies which access levels you want logged on the SMF data file. The levels you can specify are:

ALTER
logs ALTER access-level attempts only.

CONTROL
logs access attempts at the CONTROL and ALTER levels.

READ
logs access attempts at any level. READ is the default value if you omit audit-access-level.

UPDATE
logs access attempts at the UPDATE, CONTROL, and ALTER levels.

FAILURES(READ) is the default value if you omit the AUDIT operand.

DATA('*installation-defined-data*')
specifies up to 255 characters of installation-defined data to be stored in the file profile. The data must be enclosed in single quotation marks. It may also contain double-byte character set (DBCS) data.

Use the LFILE command to list this information.

FCLASS(*profile-name-2-class*)
specifies the name of the class to which *profile-name-2* belongs. The valid class names are FILE, DIRECTRY, DATASET, or other classes defined in the class descriptor table. For a list of general resource classes supplied by IBM, see Appendix B, "IBM-Supplied Resource Classes that Apply to z/VM Systems," on page 349. If you omit this operand, RACF assumes the FILE class. This operand is valid only when you also specify the FROM operand; otherwise, RACF ignores it.

FGENERIC
specifies that RACF is to treat *profile-name-2* as a generic name, even if it does not contain any generic characters. This operand is needed only if *profile-name-2* is a DATASET profile.

FROM(*profile-name-2*)
specifies the name of an existing discrete or generic profile that RACF is to use as a model for the new profile. The model profile name you specify on the FROM operand overrides any model name specified in your user or group profile. If you specify FROM and omit FCLASS, RACF assumes that *profile-name-2* is the name of a profile in the FILE class.

If FCLASS is not specified or FCLASS(FILE) is specified, *profile-name-2* must be the name of a profile in the FILE class. If FCLASS(DIRECTRY) is specified, *profile-name-2* must be the name of a profile in the DIRECTRY class. For the formats of these profile names, see "Profile Names for SFS Files and Directories" on page 342.

To specify FROM, you must have sufficient authority to both *profile-name* and *profile-name-2*, as described in "Authorization Required" on page 22.

Possible Changes to Copied Profiles When Modeling Occurs

When a profile is copied during profile modeling, the new profile could differ from the model in the following ways:

- RACF either places the user creating the new profile on the access list with ALTER access authority or, if the user is already on the access list, RACF changes the user's access authority to ALTER.
- If the SETROPTS MLS option is in effect, the security label, if specified in the model profile, is not copied. Instead, the user's current security label is used.

  EXCEPTION: When SETROPTS MLS and MLSTABLE are both in effect and the user has the SPECIAL attribute, the security label specified in the model profile is copied to the new profile.

For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

LEVEL(*nn*)
specifies a level indicator, where *nn* is an integer between 0 and 99. The default is 0.

Your installation assigns the meaning of the value.

RACF includes it in all records that log SFS file accesses and in the LFILE command display.

NOTIFY[(*userid*)]
specifies the user ID of a user to be notified whenever RACF uses this profile to deny access to a file. If you specify NOTIFY without specifying a user ID, RACF takes your user ID as the default; you will be notified whenever the profile denies access to a file.

A user who is to receive NOTIFY messages should log on frequently to take action in response to the unauthorized access attempt described in each message. RACF sends NOTIFY messages as follows to the specified user ID. If the user ID is logged on, the message immediately appears on the user's screen. If the user ID is not logged on or is disconnected, RACF sends the message to the user in a reader file. The name of this reader file will be the user ID specified on the NOTIFY keyword, and the type will be NOTIFY. (Note that you should not specify the user ID of a virtual machine that always runs disconnected.)

When the file profile also includes WARNING, RACF might have granted access to the file to the user identified in the message.

OWNER(*userid* or *group-name*)
specifies a RACF-defined user or group to be assigned as the owner of the file profile.

If you omit this operand, you are defined as the owner of the file profile.

If you specify OWNER(*userid*), the user you specify as the owner does not automatically have access to the file. Use the PERMFILE command to add the owner to the access list as desired.

SECLABEL(*security-label*)
specifies an installation-defined security label for this profile. A security label corresponds to a particular security level (such as CONFIDENTIAL) with a set of zero or more security categories (such as PAYROLL or PERSONNEL).

For a list of security labels that you are authorized to use, enter:

```
SEARCH CLASS(SECLABEL)
```

RACF stores the name of the security label you specify in the file profile if you are authorized to use that SECLABEL.

If you are not authorized to the SECLABEL or if the name you had specified is not defined as a SECLABEL profile in the SECLABEL class, the file profile is not created.

Note: If the SECLABEL class is active and the security label is specified in this profile, any security levels and categories in the profile are ignored.

SECLEVEL(*security-level*)
specifies the name of an installation-defined security level. This name corresponds to the number that is the minimum security level that a user must have to access the file. The *security-level* must be a member of the SECLEVEL profile in the SECDATA class.

When you specify SECLEVEL and the SECDATA class is active, RACF adds security level access checking to its other authorization checking. If global access checking does not grant access, RACF compares the security level allowed in the user profile with the security level required in the file profile. If the security level in the user profile is less than the security level in the file profile, RACF denies the access. If the security level in the user profile is equal to or greater than the security level in the file profile, RACF continues with other authorization checking.

If the SECDATA class is not active, RACF stores the name you specify in the file profile. When the SECDATA class is activated and the name you specified is defined as a SECLEVEL profile, RACF can perform security level access checking for the file profile. If the name you specify is not defined as a SECLEVEL profile and the SECDATA class is active, you are prompted to provide a valid *security-level*.

UACC(*access-authority*)
specifies the universal access authority to be associated with the file. The universal access authorities are ALTER, CONTROL, UPDATE, READ, and NONE. See "Access Authority for SFS Files and Directories on z/VM" on page 12 for more information.

If UACC is not specified, RACF uses the value in the ACEE or the class descriptor table. If UACC is specified without *access-authority*, RACF uses the value in the current connect group.

WARNING
specifies that, even if access authority is insufficient, RACF is to issue a warning message and allow access to the file. RACF also records the access attempt in the SMF record if logging is specified in the profile.

Examples

Example

Operation	Protect your file REPORT SCRIPT in directory SCHOOL with a discrete profile. Notify user GARYLEE if RACF denies access to the file.
Known	Your file pool ID is FP1 and your user ID is KLINE.
Command	`ADDFILE REPORT SCRIPT FP1:KLINE.SCHOOL NOTIFY(GARYLEE)`
Defaults	OWNER(KLINE) AUDIT(FAILURES(READ)) LEVEL(0)

ADDGROUP (Add Group Profile)

System environment

This command applies to both z/OS and z/VM systems.

Purpose

Use the ADDGROUP command to define a new group to RACF.

The command adds a profile for the new group to the RACF database. It also establishes the relationship of the new group to the superior group you specify.

Group profiles consist of a RACF segment and, optionally, a DFP segment and an OVM segment. You can use this command to specify information in any segment of the profile.

Related Commands

- To delete a group profile, use the DELGROUP command as described in "DELGROUP (Delete Group Profile)" on page 141.
- To change a group profile, use the ALTGROUP command as described in "ALTGROUP (Alter Group Profile)" on page 86.
- To connect a user to a group, use the CONNECT command as described in "CONNECT (Connect User to Group)" on page 128.
- To remove a user from a group, use the REMOVE command as described in "REMOVE (Remove User from Group)" on page 246.

Authorization Required

To use the ADDGROUP command, you must meet at least one of the following conditions:

- Have the SPECIAL attribute
- Have the group-SPECIAL attribute within the superior group
- Be the owner of the superior group
- Have JOIN authority in the superior group.

To add DFP or OVM suboperands to a group's profile you must meet at least one of the following conditions:

- You must have the SPECIAL attribute.
- Your installation must permit you to do so through field level access checking.

For information on field level access checking, see *z/VM: RACF Security Server Security Administrator's Guide*.

Syntax

The following operands used with the ADDGROUP command apply to z/OS systems only:

- DFP
- MODEL

The complete syntax of the command is:

ADDGROUP AG	(***group-name ...***) [DATA('*installation-defined-data*')] [OVM([GID(*group-identifier*)])] [OWNER(*userid* or *group-name*)] [SUPGROUP(*group-name*)] [TERMUACC | NOTERMUACC]
z/OS Specific Operands:	[DFP([DATAAPPL(*application-name*)] [DATACLAS(*data-class-name*)] [MGMTCLAS(*management-class-name*)] [STORCLAS(*storage-class-name*)])] [MODEL(*dsname*)]

Parameters

group-name
specifies the name of the group whose profile is to be added to the RACF database. If you are defining more than one group, the list of group names must be enclosed in parentheses.

This operand is required and must be the first operand following ADDGROUP. Each *group-name* must be unique and must not currently exist in the RACF database as a group name or a user ID.

DATA('*installation-defined-data*')
specifies up to 255 characters of installation-defined data to be stored in the group profile. It may also contain double-byte character set (DBCS) data and must be enclosed in single quotation marks.

Use the LISTGRP command to list this information.

DFP
Note: *This operand applies to z/OS systems only.*

specifies that when you define a group to RACF, you can enter any of the following suboperands to specify default values for the DFP data, management, and storage classes. DFP uses this information to determine data management and DASD storage characteristics when a user creates a new group data set.

DATAAPPL(*application-name*)
specifies an 8-character DFP data application identifier.

DATACLAS(*data-class-name*)
specifies the default data class. The maximum length of a data class name is 8 characters.

A data class can specify some or all of the physical data set attributes associated with a new data set. During new data set allocation, data management uses the value you specify as a default unless it is preempted by a higher priority default, or overridden in some other way (for example, by JCL).

Note: The value you specify must be a valid data class name defined for use on your system. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

For information on defining DFP data classes, see *MVS/Extended Architecture Storage Administration Reference*.

MGMTCLAS(*management-class-name*)
specifies the default management class. The maximum length of a management class name is 8 characters.

A management class contains a collection of management policies that apply to data sets. Data management uses the value you specify as a default unless it is preempted by a higher priority default, or overridden in some other way (for example, by JCL).

Note: The value you specify must be defined as a profile in the MGMTCLAS general resource class, and the group must be granted at least READ access to the profile. Otherwise, RACF will not allow the group access to the specified MGMTCLAS. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

For information on defining DFP management classes, see *MVS/Extended Architecture Storage Administration Reference*.

STORCLAS(*storage-class-name*)
specifies the default storage class. The maximum length of a *storage-class-name* is 8 characters.

A storage class specifies the service level (performance and availability) for data sets managed by the Storage Management Subsystem (SMS). During new data set allocation, data management uses the value you specify as a default unless it is preempted by a higher priority default, or overridden in some other way (for example, by JCL).

Note: The value you specify must be defined as a profile in the STORCLAS general resource class, and the group must be granted at least READ access to the profile. Otherwise, RACF will not allow the group access to the specified STORCLAS. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

For information on defining DFP storage classes, see *MVS/Extended Architecture Storage Administration Reference*.

MODEL(*dsname*)
Note: *This operand applies to z/OS systems only.*

MODEL specifies the name of a discrete z/OS data set profile to be used as a model for new *group-name* data sets. For this operand to be effective, the MODEL(GROUP) option (specified on the SETROPTS command) must be active.

RACF always prefixes the data set name with *group-name* when it accesses the model.

For information about automatic profile modeling, refer to *z/VM: RACF Security Server Security Administrator's Guide*.

OVM
specifies OpenExtensions information for the group being defined to RACF.

GID(*group-identifier*)
specifies the OpenExtensions group identifier. The GID is a numeric value between 0 and 2 147 483 647.

If GID is not specified, the default GID of 4 294 967 295 (X'FFFFFFFF') is assigned. The LISTGRP command displays the field name followed by the word “NONE”.

Note:

1. RACF does not require the GID to be unique. The same value can be assigned to multiple groups, but this is not recommended because individual group control would be lost. However, if you want a set of groups to have exactly the same access to the OpenExtensions resources, you may decide to assign the same GID to more than one group.
2. RACF allows you to define and connect a user to more than NGROUPS_MAX groups, but when a process is created or OpenExtensions group information is requested, only up to the first NGROUPS_MAX OpenExtensions groups will be associated with the process or user.

   The first NGROUPS_MAX OpenExtensions groups to which a user is connected, in alphabetical order, are the groups that get associated with the OpenExtensions user.

   See *z/VM: RACF Security Server Macros and Interfaces* for information on NGROUPS_MAX in the ICHNGMAX macro.

OWNER(*userid or group-name*)
specifies a RACF-defined user or group to be assigned as the owner of the new group. If you do not specify an owner, you are defined as the owner of the group. If you specify a group name, it must be the name of the superior group for the group you are adding.

SUPGROUP(*group-name*)
specifies the name of an existing RACF-defined group. This group becomes the superior group of the group profile you are defining.

If you omit SUPGROUP, RACF uses your current connect group as the superior group.

If you specify a group name and also specify OWNER with a group name, you must use the same group name on both SUPGROUP and OWNER.

If your authority to issue ADDGROUP comes from the group-SPECIAL attribute, any group you specify must be within the scope of the group in which you are a group-SPECIAL user.

TERMUACC | NOTERMUACC

TERMUACC
specifies that, during terminal authorization checking, RACF allows any user in the group access to a terminal based on the universal access authority for that terminal. TERMUACC is the default value if you omit both TERMUACC and NOTERMUACC.

NOTERMUACC
specifies that the group or a user connected to the group must be explicitly authorized (through the PERMIT command with at least READ authority) to access a terminal.

Examples

Example 1

Operation	User IA0 wants to add the group PROJECTA as a subgroup of RESEARCH. User IA0 will be the owner of group PROJECTA. Users in group PROJECTA will be allowed to access a terminal based on the universal access authority assigned to that terminal.
Known	User IA0 has JOIN authority to group RESEARCH. User IA0 is currently connected to group RESEARCH.
Command	`ADDGROUP PROJECTA`
Defaults	SUPGROUP(RESEARCH) OWNER(IA0) TERMUACC

Example 2

Operation	User ADM1 wants to add the group PROJECTB as a subgroup of RESEARCH. Group RESEARCH will be the owner of group PROJECTB. Group PROJECTB must be authorized to use terminals through the PERMIT command.
Known	User ADM1 has JOIN authority to group RESEARCH. User ADM1 is currently connected to group SYS1.
Command	`ADDGROUP PROJECTB SUPGROUP(RESEARCH) OWNER(RESEARCH) NOTERMUACC`
Defaults	None

ADDGROUP Examples on z/OS

Example 3

Operation: User ADM1 wants to add the group SYSINV as a subgroup of RESEARCH. This group will be used as the administrative group for RACF and will use a model name of 'SYSINV.RACF.MODEL.PROFILE'.

Known: User ADM1 has JOIN authority to group RESEARCH.

Command:

```
ADDGROUP SYSINV SUPGROUP(RESEARCH)
MODEL(RACF.MODEL.PROFILE) DATA('RACF
ADMINISTRATION GROUP')
```

Defaults: OWNER(ADM1) TERMUACC

Example 4

Operation: User ADM1 wants to add the group DFPADMN as a subgroup of SYSADMN. Group SYSADMN will be the owner of group DFPADMN. Users in group DFPADMN will be allowed to access a terminal based on the universal access authority assigned to that terminal. Group DFPADMN will be assigned the following default information to be used for new DFP-managed data sets created for the group:

- Data class DFP2DATA
- Management class DFP2MGMT
- Storage class DFP2STOR
- Data application identifier DFP2APPL.

Known:

- User ADM1 has JOIN authority to group SYSADMN.
- User ADM1 is currently connected to group SYS1.
- User ADM1 has field level access of ALTER to the fields in the DFP segment.
- DFP2MGMT has been defined to RACF as a profile in the MGMTCLAS general resource class, and group DFPADMN has been given READ access to this profile.
- DFP2STOR has been defined to RACF as a profile in the STORCLAS general resource class, and group DFPADMN has been given READ access to this profile.

Command:

```
ADDGROUP DFPADMN SUPGROUP(SYSADMN)
OWNER(SYSADMN) DFP(DATACLAS(DFP2DATA)
MGMTCLAS(DFP2MGMT) STORCLAS(DFP2STOR)
DATAAPPL(DFP2APPL))
```

Defaults: TERMUACC

ADDSD (Add Data Set Profile)

System environment

Data sets apply to z/OS systems only.

Purpose

Use the ADDSD command to RACF-protect data sets with either discrete or generic profiles. For additional information, see “Profile Names for Data Sets” on page 336.

Changes made to discrete profiles take effect after the ADDSD command is processed. Changes made to generic profiles do not take effect until one or more of the following steps is taken:

- The user of the data set issues the LISTDSD command:

```
LISTDSD DA(data-set-protected-by-the-profile) GENERIC
```

  Note: Use the data set name, not the profile name.
- The security administrator issues the SETROPTS command:

```
SETROPTS GENERIC(DATASET) REFRESH
```

  See SETROPTS command for authorization requirements.
- The user of the data set logs off and logs on again.

For more information, refer to *z/VM: RACF Security Server Security Administrator's Guide*.

Note: RACF interprets dates with 2 digit years in the following way, YY represents the 2 digit year.

```
     IF 70 < YY <= 99 THEN
        The date is interpreted as 19YY
     IF 00 <= YY <= 70 THEN
        The date is interpreted as 20YY
```

Related Commands

- To change a data set profile, use the ALTDSD command as described in “ALTDSD (Alter Data Set Profile)” on page 71.
- To delete a data set profile, use the DELDSD command as described in “DELDSD (Delete Data Set Profile)” on page 136.
- To permit or deny access to a data set profile, use the PERMIT command as described in “PERMIT (Maintain Resource Access Lists)” on page 202.

Authorization Required

The level of authority you need to use the ADDSD command and the types of profiles you can define are:

- To protect one or more user data sets with RACF, one of the following must be true:
  - The high-level qualifier of the data set name (or the qualifier supplied by the RACF naming conventions table or by a command installation exit) must match your user ID.
  - You must have the SPECIAL attribute.
  - The user ID for the data set profile must be within the scope of a group in which you have the group-SPECIAL attribute.

You may not protect a user data set for someone else (the high-level qualifier or installation-supplied qualifier is not your user ID) unless you have the SPECIAL attribute or the data set profile is within the scope of a group in which you have the group-SPECIAL attribute.

Note: You need not have the SPECIAL attribute to specify the OWNER operand.

- To protect a group data set with RACF, one of the following must be true:
  - You must have at least CREATE authority in the group.
  - You must have the SPECIAL attribute.
  - You must have the OPERATIONS attribute and not be connected to the group.
  - The data set profile must be within the scope of the group in which you have the group-SPECIAL attribute.
  - The data set profile must be within the scope of the group in which you have the group-OPERATIONS attribute, and you must not be connected to the group.

  Note:

  1. If you have the OPERATIONS or group-OPERATIONS attribute and are connected to a group, you must have at least CREATE authority in that group to protect a group data set.
  2. To protect a group data set where the high-level qualifier of the data set name is VSAMDSET, you need neither CREATE authority in the VSAMDSET group nor the SPECIAL attribute. (A universal group authority of CREATE applies to the RACF-defined VSAMDSET group.)
- To define to RACF a data set that was brought from another system where it was RACF-indicated and RACF-protected with a discrete profile, either
  - You must either have the SPECIAL attribute, or the data set's profile is within the scope of a group in which you have the group-SPECIAL attribute,

    or
  - Your user ID must be the high-level qualifier of the data set name (or the qualifier supplied by the naming conventions routine or a command installation exit).
- To assign a security category to a profile, you must have the SPECIAL attribute or have the category in your user profile.
- To assign a security level to a profile, you must have the SPECIAL attribute or, in your own profile, a security level that is equal to or greater than the security level you are defining.
- To assign a security label to a profile, you must have the SPECIAL attribute or READ authority to the security label profile. However, the security administrator can limit the ability to assign security labels to only users with the SPECIAL attribute.
- To access the DFP segment, field level access checking is required.
- When either a user or group uses modeling to protect a data set with a discrete profile, RACF copies the following fields from the model profile: the level number, audit flags, global audit flags, the universal access authority (UACC), the owner, the warning, the access list, installation data, security category names, the security level name, the user to be notified, the retention period for a tape data set, and the erase indicator.
- To add a discrete profile for a VSAM data set already RACF-protected by a generic profile, you must have ALTER access authority to the catalog or to the data set through the generic profile.

Model Profiles

To specify a model data set profile (using, as required, FROM, FCLASS, FGENERIC, and FVOLUME), you must have sufficient authority over the model profile — the “from” profile. RACF makes the following checks until one of the conditions is met:

- You have the SPECIAL attribute.
- The “from” profile is within the scope of a group in which you have the group-SPECIAL attribute.
- You are the owner of the “from” profile.

- The high-level qualifier of the profile name (or the qualifier supplied by the naming conventions routine or a command installation exit routine) is your user ID.

For discrete profiles only:

- You are on the access list in the "from" profile with ALTER authority. (If you have any lower level of authority, you cannot use the profile as a model.)
- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is on the access list in the "from" profile with ALTER authority. (If any group that RACF checked has any lower level of authority, you may not use the profile as a model.)
- The UACC is ALTER.

Syntax

The complete syntax of the ADDSD command is:

```
ADDSD                (profile-name-1 [/password] ...)
AD                   [ ADDCATEGORY(category-name ...) ]
                     [ AUDIT( access-attempt [(audit-access-level)] ...) ]
                     [ DATA('installation-defined-data') ]
                     [ DFP(RESOWNER(userid or group-name)) ]
                     [ ERASE ]
                     [ FCLASS(profile-name-2-class) ]
                     [ FGENERIC ]
                     [ FILESEQ(number) ]
                     [ FROM(profile-name-2) ]
                     [ FVOLUME(profile-name-2-serial) ]
                     [ {GENERIC | MODEL | TAPE} ]
                     [ LEVEL(nn) ]
                     [ {NOSET | SET | SETONLY} ]
                     [ NOTIFY [(userid) ] ]
                     [ OWNER(userid or group-name) ]
                     [ RETPD(nnnnn) ]
                     [ SECLABEL(security-label) ]
                     [ SECLEVEL(security-level) ]
                     [ UACC(access-authority) ]
                     [ UNIT(type) ]
                     [ VOLUME(volume-serial ...) ]
                     [ WARNING ]
```

Parameters

profile-name-1
specifies the name of the discrete or generic profile to be added to the RACF database. If you specify more than one name, the list of names must be enclosed in parentheses.

The high-level qualifier of the profile name (or the qualifier determined by the naming conventions table or by a command installation exit) must be either a user ID or group name. To specify a user ID other than your own, you must have the SPECIAL attribute, or the data set profile must be within the scope of a group in which you have the group-SPECIAL attribute. To define a group data set where the high-level qualifier of the data set name is not VSAMDSET, you must have at least CREATE authority in the specified group, or the SPECIAL attribute, or the data set must be within the scope of a group in which you have the group-SPECIAL attribute.

This operand is required and must be the first operand following ADDSD. Note that, because RACF uses the RACF database and not the system catalog, you cannot use alias data set names.

For additional information, see "Profile Names for Data Sets" on page 336 and the section describing rules for defining data set profiles in *z/VM: RACF Security Server Security Administrator's Guide*.

OS CVOL: If you are protecting an OS CVOL, use the naming convention SYSCTLG.Vxxxxxx, where xxxxxx represents the volume serial number for the volume containing the CVOL.

VSAM Data Set: If your data management does not include support for always-call, a VSAM data set must be cataloged in a catalog that is also RACF-protected in order for the data set to be RACF-protected.

Tape Data Set: If you are defining a discrete profile that protects a tape data set, you must specify TAPE. If you are defining more than one tape data set profile, the data sets must all reside on the same volume, and you must specify the profile names in an order that corresponds to the file sequence numbers of the data sets on the volume.

Note: Do not specify a generic character unless SETROPTS GENERIC (or SETROPTS GENCMD) is in effect.

/password
specifies the data set password if you are protecting an existing password-protected data set. If you specify a generic or model profile, RACF ignores this operand.

For a non-VSAM password-protected data set, the WRITE level password must be specified.

For a VSAM password-protected data set, one of the following conditions must exist:

- The MASTER level password for the data set must be specified
- If the catalog containing the entry for the data set is RACF-protected, then you must have ALTER access to the catalog
- If the catalog containing the entry for the data set is not RACF-protected, but is password-protected, then the MASTER level password for the catalog must be specified.

For a VSAM data set that is not password-protected, you do not need the password or RACF access authority for the catalog.

A password is not required when you specify NOSET.

If the command is executing in the foreground and you omit the password for a password-protected data set, the logon password is used. You are prompted if the password you enter or the logon password is incorrect. (If it is a non-VSAM multivolume data set, you are prompted once for each volume on which the data set resides.)

If the command is executing in a batch job and you either omit the password for a password-protected data set or supply an incorrect password, the operator is prompted. (If it is a non-VSAM multivolume data set, the operator is prompted once for each volume on which the data set resides.)

ADDCATEGORY(*category-name ...*)
specifies one or more names of installation-defined security categories. The names you specify must be defined as members of the CATEGORY profile in SECDATA class. (For information on defining security categories, see *z/VM: RACF Security Server Security Administrator's Guide*.)

When the SECDATA class is active and you specify ADDCATEGORY, RACF performs security category checking in addition to its other authorization checking. If a user requests access to a data set, RACF compares the list of security categories in the user's profile with the list of security categories in the data set profile. If RACF finds any security category in the data set profile that is not in the user's profile, RACF denies access to the data set. If the user's profile contains all the required security categories, RACF continues with other authorization checking.

Note: RACF does not perform security category checking for a started procedure with the privileged attribute.

When the SECDATA class is not active, RACF ignores this operand. When the CATEGORY profile does not include a member for a category-name, you are prompted to provide a valid category-name.

AUDIT(*access-attempts*(*audit-access-level*)...)

access-attempts
specifies which access attempts you want to log on the SMF data set. The following options are available:

ALL
indicates that you want to log both authorized accesses and detected unauthorized access attempts.

FAILURES
indicates that you want to log detected unauthorized attempts.

NONE
indicates that you do not want any logging to be done.

SUCCESS
indicates that you want to log authorized accesses.

audit-access-level
specifies which access levels you want logged on the SMF data set. The levels you can specify are:

ALTER
logs ALTER access-level attempts only.

CONTROL
logs access attempts at the CONTROL and ALTER levels.

READ
logs access attempts at any level. READ is the default value if you omit audit-access-level.

UPDATE
logs access attempts at the UPDATE, CONTROL, and ALTER levels.

FAILURES(READ) is the default value if you omit the AUDIT operand. You cannot audit access attempts at the EXECUTE level.

DATA('*installation-defined-data*')
specifies up to 255 characters of installation-defined data to be stored in the data set profile. It may also contain double-byte character set (DBCS) data and must be enclosed in single quotation marks.

Use the LISTDSD command to list this information. It is available to the RACF postprocessing installation exit routine for RACHECK. If the profile is a model profile, the information is copied to the installation-defined data area for new profiles.

DFP
specifies that, for an SMS-managed data set, you can enter the following information:

RESOWNER(*userid* or *group-name*)
specifies the user ID or group name of the actual owner of the data sets protected by the profile specified in *profile-name-1*. This name must be that of a RACF-defined user or group. (The data set resource owner, specified with RESOWNER, is distinguished from the owner specified with OWNER, which represents the user or group that owns the data set profile).

ERASE
specifies that, when SETROPTS ERASE(NOSECLEVEL) is active, data management is to physically erase the DASD data set extents at the time the data set is deleted (scratched) or released for reuse. Erasing the data set means overwriting all allocated extents with binary zeros.

This operand is ignored for the following:

- If the data set is not a DASD data set
- If SETROPTS ERASE(ALL) is specified for your installation (user and data set profile definitions are overridden)
- SETROPTS ERASE(SECLEVEL(*security_level*)) is specified for your installation (data sets equal or higher in security level are always erased, while those lower in security level are never erased)

FCLASS(*profile-name-2-class*)
specifies the name of the class to which *profile-name-2* belongs. The valid class names are DATASET and those classes defined in the class descriptor table. If you omit this operand, RACF assumes the DATASET class. This operand is valid only when you also specify the FROM operand; otherwise, RACF ignores it.

FGENERIC
specifies that RACF is to treat *profile-name-2* as a generic name, even if it is fully qualified (meaning that it does not contain any generic characters). This operand is only needed when *profile-name-2* is a DATASET profile.

FILESEQ(*number*)
specifies the file sequence number for a tape data set. The number can range from 1 through 9999.

If you specify more than one *profile name*, RACF assigns the file sequence number that you specify to the first profile name, then increments the number by one for each additional name. Thus, be sure to specify profile names in the order of their file sequence numbers.

If you omit FILESEQ and specify VOLUME, the default is FILESEQ(1). If you omit both FILESEQ and VOLUME, RACF retrieves the file sequence number and volume serial number from the catalog.

If you omit TAPE, RACF ignores FILESEQ.

FROM(*profile-name-2*)
specifies the name of an existing discrete or generic profile that RACF is to use as a model for the new profile. The model profile name you specify on the FROM operand overrides any model name specified in your user or group profile. If you specify FROM and omit FCLASS, RACF assumes that *profile-name-2* is the name of a profile in the DATASET class.

To specify FROM, you must have sufficient authority to both *profile-name-1* and *profile-name-2*, as described in “Authorization Required” on page 33.

Naming conventions processing affects *profile-name-2* in the same way that it affects *profile-name-1*.

If the profile being added is for a group data set and the user has the GRPACC attribute for that group, RACF places the group on the access list with UPDATE access authority. Otherwise, if the group is already on the access list, RACF changes the group's access authority to UPDATE.

Possible Changes to Copied Profiles When Modeling Occurs

When a profile is copied during profile modeling, the new profile could differ from the model in the following ways:

- RACF places the user on the access list with ALTER access authority or, if the user is already on the access list, changes the user's access authority to ALTER.

  If the profile being added is for a group data set and the user has the GRPACC attribute for that group, RACF places the group on the access list with UPDATE access authority. Otherwise, if the group is already on the access list, RACF changes the group's access authority to UPDATE. These access list changes do not occur if the data set profile is created only because the user has the OPERATIONS attribute.
- The security label, if specified in the model profile, is not copied. Instead, the user's current security label is used.
- Information in the non-RACF segments (for example, the DFP segment) is not copied.

FVOLUME(*profile-name-2-serial*)
specifies the volume RACF is to use to locate the model profile (*profile-name-2*).

If you specify FVOLUME and RACF does not find *profile-name-2* associated with that volume, the command fails. If you omit this operand and the data set name appears more than once in the RACF database, the command fails.

FVOLUME is valid only when FCLASS either specifies or defaults to DATASET and when *profile-name-2* specifies a discrete profile. Otherwise, RACF ignores FVOLUME.

GENERIC | MODEL | TAPE

GENERIC
specifies that RACF is to treat *profile-name-1* as a fully qualified generic name, even if it does not contain any generic characters.

MODEL
specifies that you are defining a model profile to be used when new data sets are created. The SETROPTS command (specifying MODEL operand with either GROUP or USER) controls whether this profile is used for data sets with group names or user ID names.

When you specify MODEL, you can omit UNIT and VOLUME, and you must omit SET, NOSET, GENERIC, and TAPE.

MODEL and GENERIC keywords are mutually exclusive. These keywords specified together invalidate each other, but a generic (not fully qualified by the GENERIC keyword) profile can be used as a model profile.

For information about automatic profile modeling, refer to *z/VM: RACF Security Server Security Administrator's Guide*.

TAPE
specifies that the data set profile is to protect a tape data set. If tape data set protection is not active, RACF treats TAPE as an invalid operand and issues an appropriate error message. If *profile-name-1* is a generic profile name, RACF ignores this operand. (RACF processes a tape data set protected by a generic profile in the same way as it processes a DASD data set protected by a generic profile.)

LEVEL(*nn*)
specifies a level indicator, where *nn* is an integer between 0 and 99. The default is 0.

Your installation assigns the meaning of the value. It is not used by the authorization function in RACHECK but is available to the RACF postprocessing installation exit routine for the RACHECK SVC.

RACF includes it in all records that log data set accesses and in the LISTDSD command display.

NOSET | SET | SETONLY

NOSET
specifies that the data set is not to be RACF-indicated.

For a DASD data set, use NOSET when you are defining a data set to RACF that has been brought from another system where it was RACF-protected. (The data set is already RACF-indicated.)

For a tape data set, use NOSET when, because of a previous error, the TVTOC indicates that the data set is RACF-indicated, but the discrete profile is missing.

If you specify NOSET when the data set is not already RACF-indicated, RACF access control to that data set is not enforced.

If you specify NOSET, the volumes on which the data set or catalog resides need not be online, and the password in the first operand of this command is not required.

To use NOSET, one of the following must be true:

- You must have the SPECIAL attribute
- The profile must fall within the scope of a group in which you have the GROUP-special attribute
- The high-level qualifier of the data set name (or the qualifier supplied by a command installation exit routine) must be your user ID.

If you specify a generic profile name, RACF ignores this operand.

Note: If you specify a profile name that exists as a generation data group (GDG) data set base name with NOSET—but do not specify a unit and volume, RACF creates a model profile for the data

set instead of a discrete profile. In this situation, the model profile provides the same protection as a discrete profile.

SET
specifies that the data set is to be RACF-indicated. SET is the default value when you are RACF-protecting a data set. If the indicator is already on, the command fails. If you specify a generic profile name or the GENERIC operand, RACF ignores this operand. SET is not valid with RACF for z/VM.

SETONLY
specifies that, for a tape data set, RACF is to create only an entry in the TVTOC; it is not to create a discrete data set profile. Specifying SETONLY allows you to protect a tape data set with a TVTOC and a generic profile.

Thus, you would normally specify SETONLY with TAPE, and, when you do, RACF ignores the OWNER, UACC, AUDIT, DATA, WARNING, LEVEL, and RETPD operands. If you specify SETONLY without TAPE, RACF treats SETONLY as SET.

NOTIFY[(*userid*)]
specifies the user ID of a RACF-defined user to be notified whenever RACF uses this profile to deny access to a data set. If you specify NOTIFY without *userid*, RACF takes your user ID as the default; you are notified whenever the profile denies access to a data set.

A user who is to receive NOTIFY messages should log on frequently, both to take action in response to the unauthorized access attempts the messages describe and to clear the messages from the SYS1.BRODCAST data set. (When the profile also includes WARNING, RACF might have granted access to the data set to the user identified in the message.)

OWNER(*userid* or *group-name*)
specifies a RACF-defined user or group to be assigned as the owner of the data set profile. When you define a group data set, the user you designate as owner must have at least USE authority in the group specified by the high-level qualifier of the data set name (or the qualifier determined by the naming conventions routine or by a command installation exit routine).

If you omit this operand, you are defined as the owner of the data set profile. However, if the high level qualifier is a user ID and the user ID is different from your user ID, the OWNER of the profile will be that (high level qualifier) user ID. If you have the SPECIAL attribute and define a profile for a group data set, your user ID is added to the access list for the data set with ALTER access authority, whether or not you specify the OWNER operand. If you have the SPECIAL attribute and define a profile for a user data set, your user ID is not added to the access list for the data set.

If you specify OWNER(*userid*), the user you specify as the owner does not automatically have access to the data set. Use the PERMIT command to add the owner to the access list as desired. If you specify OWNER(*group-name*), RACF treats any users who have the group-SPECIAL attribute in the group as owners of the data set profile.

RETPD(*nnnnn*)
specifies the RACF security retention period for a tape data set. The security retention period is the number of days that must elapse before a tape data set profile expires. (Note that, even though the data set profile expires, RACF-protection for data sets protected by the profile is still in effect. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.)

The number you specify, *nnnnn* must be one to five digits in the range of 0 through 65533. To indicate a data set that never expires, specify *nnnnn* as 99999.

The RACF security retention period is the same as the data set retention period specified by the EXPDT/RETPD parameters on the JCL DD statement only when the data set profile is discrete and you do not modify the RACF security retention period.

When the TAPEVOL class is active, RACF checks the RACF security retention period before it allows a data set to be overwritten. RACF adds the number of days in the retention period to the creation date for the data set. If the result is less than the current date, RACF continues to protect the data set.

When the TAPEVOL class is not active, RACF ignores the RETPD operand.

If you omit RETPD and your installation has established a default security retention period (through the RETPD operand on the SETROPTS command), RACF uses the default. If you omit RETPD and your installation has not established a default, RACF uses 0 as a default.

Specifying this operand for a DASD data set does not cause an error, but it has no meaning because RACF ignores the operand during authorization checking.

SECLABEL(*security-label*)
specifies the user's default security label, where *security-label* is an installation-defined security label name that represents an association between a particular security level and a set of zero or more categories.

A security label corresponds to a particular security level (such as CONFIDENTIAL) with a set of zero or more security categories (such as PAYROLL or PERSONNEL).

For a list of security labels that you are authorized to use, enter:

```
SEARCH CLASS(SECLABEL)
```

RACF stores the name of the security label you specify in the data set profile if you are authorized to use that label.

If you are not authorized to use the security label or if the name you had specified is not defined as a SECLABEL profile in the SECLABEL class, the data set profile is not created.

SECLEVEL(*security-level*)
specifies the name of an installation-defined security level. This name corresponds to the number that is the minimum security level a user must have to access the data set. *security-level* must be a member of the SECLEVEL profile in the SECDATA class.

When you specify SECLEVEL and the SECDATA class is active, RACF adds security level access checking to its other authorization checking. If global access checking does not grant access, RACF compares the security level allowed in the user profile with the security level required in the data set profile. If the security level in the user profile is less than the security level in the data set profile, RACF denies the access. If the security level in the user profile is equal to or greater than the security level in the data set profile, RACF continues with other authorization checking.

Note: RACF does not perform security level checking for a started procedure with the privileged attribute.

If the SECDATA class is not active, RACF stores the name you specify in the data set profile. When the SECDATA class is activated and the name you specified is defined as a SECLEVEL profile, RACF can perform security level access checking for the data set profile. If the name you specify is not defined as a SECLEVEL profile and the SECDATA class is active, you are prompted to provide a valid name for *security-level*.

UACC(*access-authority*)
specifies the universal access authority to be associated with the data sets. The universal access authorities are ALTER, CONTROL, UPDATE, READ, EXECUTE, and NONE. If you omit UACC or specify UACC with no access authority, RACF uses the default value in your current connect group. If you specify CONTROL for a tape data set or a non-VSAM DASD data set, RACF treats the access authority as UPDATE. If you specify EXECUTE for a tape data set, or a DASD data set not used as a program library, RACF treats the access authority as NONE.

UNIT(*type*)
specifies the unit type on which a tape data set or a non-VSAM DASD data set resides. You may specify an installation-defined unit name, a generic device type, or a specific device address. If you specify UNIT and VOLUME for a DASD data set, RACF assumes that the data set is a non-VSAM data set; therefore, do not use UNIT and VOLUME for a VSAM data set.

If the data set is not cataloged, UNIT and VOLUME are required. You must specify UNIT and VOLUME for data sets cataloged with an esoteric name (such as an installation-defined unit name).

If you specify a generic or model profile name, RACF ignores this operand.

VOLUME(*volume-serial* ...)
specifies the volumes on which a tape data set or a non-VSAM DASD data set resides. If you specify UNIT and VOLUME for a DASD data set, RACF assumes that the data set is a non-VSAM data set; therefore, do not use UNIT and VOLUME for a VSAM data set.

If the data set is not cataloged, UNIT and VOLUME are required. You must specify UNIT and VOLUME for data sets cataloged with an esoteric name (such as an installation-defined unit name).

If you specify a tape data set profile name, you may specify only one volume.

If you specify a generic or model profile name, RACF ignores this operand.

WARNING
specifies that, even if access authority is insufficient, RACF is to issue a warning message and allow access to the resource. RACF also records the access attempt in the SMF record if logging is specified in the profile.

Examples

Example 1

Operation: User ADM1 wants to create a generic profile to protect all data sets having the high-level qualifier SALES. Only users with a security level of CONFIDENTIAL or higher are to be able to access the data sets.

Known: User ADM1 has the SPECIAL attribute, the operating system has data management always-call, and the installation has defined CONFIDENTIAL as a valid security level name.

Command:
```
ADDSD 'SALES.*' UACC(READ) AUDIT(ALL(READ))
SECLEVEL(CONFIDENTIAL)
```

Defaults: OWNER(ADM1) LEVEL(0)

Example 2

Operation: User AEH0 wants to protect the data set AEH0.DEPT1.DATA with a discrete RACF profile.

Known: User AEH0 is RACF-defined. AEH0.DEPT1.DATA is not cataloged. It resides on volume USER03 which is a 3330 volume.

Command:
```
ADDSD 'AEH0.DEPT1.DATA' UNIT(3330)
VOLUME(USER03)
```

Defaults: OWNER(AEH0) UACC(UACC of user AEH0 in current connect group) AUDIT(FAILURES(READ)) LEVEL(0) SET

Example 3

Operation: User ADM1 wants to RACF-define the DASD data set SYS1.ICH02.DATA which was brought from another system where it was protected by a discrete RACF profile and was RACF-indicated. On the new system, only users with a security category of DEPT1 are to be allowed to access the data set.

Known: User ADM1 has the SPECIAL attribute. SYS1.ICH02.DATA is cataloged. User ADM1 has create authority in group SYS1 and is connected to group SYS1 with the group-SPECIAL attribute. The installation has defined DEPT1 as a valid security category.

Command:
```
ADDSD 'SYS1.ICH02.DATA' OWNER(SYS1) UACC(NONE)
AUDIT(ALL) NOSET CATEGORY(DEPT1)
```

Defaults: LEVEL(0)

Example 4

Operation: User AEHO wants to create a model profile for group RSC and place an installation-defined description in the profile.

Known: User AEHO has at least CREATE authority in group RSC.

Command:
```
ADDSD 'RSC.ACCESS.PROFILE' MODEL DATA('PROFILE
THAT CONTAINS MODELING INFORMATION')
```

Defaults: OWNER(AEHO), UACC(the UACC of user AEHO in current group) AUDIT(FAILURES(READ)) LEVEL(0)

Example 5

Operation: User AEH1 wants to protect the tape data set named AEH1.TAPE.RESULTS with a discrete RACF profile.

Known: User AEH1 is a RACF-defined user. Data set AEH1.TAPE.RESULTS is cataloged, and tape data set protection is active.

Command:
```
ADDSD 'AEH1.TAPE.RESULTS' UACC(NONE)
AUDIT(ALL(READ)) TAPE NOTIFY FILESEQ(1)
RETPD(100)
```

Defaults: LEVEL(0)

Example 6

Operation: User AEH1 wants to protect the tape data set named AEH1.TAPE.FUTURES with a discrete RACF profile, which is so much like the profile created for AEH1.TAPE.RESULTS (Example 5) that AEH1 can use the existing profile as a model for the new profile.

Known: User AEH1 is a RACF-defined user. Data set AEH1.TAPE.FUTURES is cataloged, and tape data set protection is active.

Command:
```
ADDSD 'AEH1.TAPE.FUTURES'
FROM('AEH1.TAPE.RESULTS') FILESEQ(2)
```

Defaults: LEVEL(0)

Example 7

Operation: User ADM1 wants to create a generic profile to protect all data sets having the high-level qualifier PROJECTA. The data sets protected by the profile will be managed by DFP. Group TEST4 will be assigned as the actual owner of the data sets protected by the profile. The profile will have a universal access authority of READ.

Known: User ADM1 has the SPECIAL attribute, the operating system has DFP 3.1.0 installed, and TEST4 is a RACF-defined group.

Command:
```
ADDSD 'PROJECTA.*' UACC(READ)
DFP(RESOWNER(TEST4))
```

Defaults: OWNER(ADM1) LEVEL(0) AUDIT(FAILURES(READ))

Example 8

Operation: User TSO7 wants to create a generic profile to protect all data sets having the high-level qualifier PROJECTB with a security label of CONF. User TSO7 is authorized to the security label.

Known: User TSO7 is a RACF-defined user.

Command:
```
ADDSD 'PROJECTB.*' SECLABEL(CONF)
```

Defaults: None

ADDUSER (Add User Profile)

System environment

This command applies to both z/OS and z/VM systems.

Purpose

Use the ADDUSER command to define a new user to RACF and establish the user's relationship to an existing RACF-defined group.

The command adds a profile for the new user to the RACF data base and connects the user to the default group you specify.

The user profile consists of a RACF segment and, optionally, other segments such as a TSO segment, a DFP segment, or an OVM segment. You can use this command to define information in any segment of the user's profile.

ADDUSER creates a user ID without a password, without a password phrase, and without Multi-Factor Authentication (MFA), unless values are explicitly assigned. Such a user ID can be the target of an XAUTOLOG, or a LOGON BY, but cannot be directly logged on. You can choose to assign only a password, only a password phrase, only MFA, or any combination of the three, depending on your policy.

Related Commands

- To change a user profile, use the ALTUSER command as described in “ALTUSER (Alter User Profile)” on page 93.
- To delete a user profile, use the DELUSER command as described in “DELUSER (Delete User Profile)” on page 143.
- To list a user profile, use the LISTUSER command as described in “LISTUSER (List User Profile)” on page 179.
- To enter a command containing a long pathname, use the RAC command as described in “RAC (Enter RACF Commands on z/VM)” on page 207.

Authorization Required

To use the ADDUSER command, you must have one of the following:

- The SPECIAL attribute
- The CLAUTH attribute for the USER class while one of the following is true:
  - You are the owner of the default group specified in this command
  - You have JOIN authority in the default group specified in this command
  - The default group is within the scope of a group in which you have the group-SPECIAL attribute.

You must have the SPECIAL attribute to give the new user the OPERATIONS, SPECIAL, AUDITOR, or ROAUDIT attribute. You need not, however, have the SPECIAL attribute to specify the OWNER operand.

You cannot assign a user an attribute or authority higher than your own.

To assign a security category to a profile, you must have the SPECIAL attribute, or the category must be in your user profile. To assign a security level to a profile, you must have the SPECIAL attribute or, in your own profile, a security level that is equal to or greater than the security level you are assigning.

To assign a security label, you must have the SPECIAL attribute or have READ authority to the security label profile. However, the security administrator can limit the ability to assign security labels only to users with the SPECIAL attribute.

To define information within a segment other than the RACF segment (such as the TSO, DFP, OVM, or other segments), you must have one of the following:

- The SPECIAL attribute
- At least UPDATE authority to the desired field within the segment through field level access control.

For information on field level access checking, see *z/VM: RACF Security Server Security Administrator's Guide*.

Syntax

The following operands used with the ADDUSER command apply to z/OS systems only:

- ADSP | NOADSP
- CICS
- DFP
- GRPACC | NOGRPACC
- LANGUAGE
- MODEL
- OPERPARM
- TSO
- WORKATTR.

The complete syntax of the command is:

```
ADDUSER          (userid ...)
AU               [ ADDCATEGORY(category-name ...) ]
                 [ AUDITOR | NOAUDITOR ]
                 [ AUTHORITY(group-authority) ]
                 [ CLAUTH(class-name ...) | NOCLAUTH ]
                 [ DATA('installation-defined-data') ]
                 [ DFLTGRP(group-name) ]
                 [ MFA([ PWFALLBACK | NOPWFALLBACK ] ) | NOMFA ]
                 [ NAME('user-name') ]
                 [ OPERATIONS | NOOPERATIONS ]
                 [ OVM(
                   [ FSROOT(file-system-root) ]
                   [ HOME(initial-directory-name) ]
                   [ PROGRAM(program-name) ]
                   [ UID(user-identifier) ]
                   ) ]
                 [ OWNER(userid or group-name) ]
                 [ PASSWORD(password) | NOPASSWORD ]
                 [ PHRASE('password phrase') ]
                 [ ROAUDIT | NOROAUDIT ]
                 [ SECLABEL(seclabel-name) ]
                 [ SECLEVEL(seclevel-name) ]
                 [ SPECIAL | NOSPECIAL ]
                 [ UACC(access-authority) ]
                 [ WHEN( [DAYS(day-info)] [TIME(time-info)] ) ]
```

z/OS Specific Operands:

[ADSP | NOADSP]
[CICS(
  [OPCLASS(*operator-class1,operator-class2,...*)]
  [OPIDENT(*operator-id*)]
  [OPPRTY(*operator-priority*)]
  [TIMEOUT(*timeout-value*)]
  [XRFSOFF(FORCE | NOFORCE)]
)]
[DFP(
  [DATAAPPL(*application-name*)]
  [DATACLAS(*data-class-name*)]
  [MGMTCLAS(*management-class-name*)]
  [STORCLAS(*storage-class-name*)]
)]
[GRPACC | NOGRPACC]
[LANGUAGE(
  [PRIMARY(*language*)]
  [SECONDARY(*language*)]
)]
[MODEL(*dsname*)]
[OPERPARM(
  [ALTGRP(*alternate-console-group*)]
  [AUTH(*operator-authority*)]
  [AUTO(YES | NO)]
  [CMDSYS(*system-name*)]
  [DOM(NORMAL | ALL | NONE)]
  [KEY(*searching-key*)]
  [LEVEL(*message-level*)]
  [LOGCMDRESP(SYSTEM | NO)]
  [MFORM(*message-format*)]
  [MIGID(YES | NO)]
  [MONITOR(*event*)]
  [MSCOPE(*system-names* | * | *ALL)]
  [ROUTCODE(ALL | NONE | *routing-codes*)]
  [STORAGE(*amount*)]
  [UD(YES | NO)]
)]
[TSO(
  [ACCTNUM(*account-number*)]
  [DEST(*destination-id*)]
  [HOLDCLASS(*hold-class*)]
  [JOBCLASS(*job-class*)]
  [MAXSIZE(*maximum-region-size*)]
  [MSGCLASS(*message-class*)]
  [PROC(*logon-procedure-name*)]
  [SECLABEL(*security-label*)]
  [SIZE(*default-region-size*)]
  [SYSOUTCLASS(*sysout-class*)]
  [UNIT(*unit-name*)]
  [USERDATA(*user-data*)]
)]

```
[ WORKATTR(
  [ WAACCNT(account-number) ]
  [ WAADDR1(address-line-1) ]
  [ WAADDR2(address-line-2) ]
  [ WAADDR3(address-line-3) ]
  [ WAADDR4(address-line-4) ]
  [ WABLDG(building) ]
  [ WADEPT(department) ]
  [ WANAME(name) ]
  [ WAROOM(room) ]
  ) ]
```

Parameters

userid
specifies the user to be defined to RACF. If you are defining more than one user, the list of user IDs must be enclosed in parentheses.

This operand is required and must be the first operand following ADDUSER.

Each user ID must be unique and must not currently exist on the RACF database as a user ID or a group name.

ADDCATEGORY(*category-name ...*)
specifies one or more names of installation-defined security categories. The names you specify must be defined as members of the CATEGORY profile in a SECDATA class. (For information on defining security categories, see *z/VM: RACF Security Server Security Administrator's Guide*.)

When the SECDATA class is active and you specify ADDCATEGORY, RACF performs security category checking in addition to its other authorization checking. If a user requests access to a resource, RACF compares the list of security categories in the user's profile with the list of security categories in the resource profile. If RACF finds any security category in the resource profile that is not in the user's profile, RACF denies access to the resource. If the user's profile contains all the required security categories, RACF continues with other authorization checking.

Note: RACF does not perform security category checking for a started procedure with the privileged attribute.

When the SECDATA class is not active, RACF ignores this operand. When the CATEGORY profile does not include a member for *category-name*, you are prompted to provide a valid name.

ADSP | NOADSP
Note: *These operands apply to z/OS systems only.*

ADSP
specifies that all permanent tape and DASD data sets created by the new user will automatically be RACF-protected by discrete profiles. ADSP specified on the ADDUSER command overrides NOADSP specified on the CONNECT command.

If SETROPTS NOADSP is in effect, RACF ignores the ADSP attribute at logon or job initiation.

NOADSP
specifies that the new user is not to have the ADSP attribute. NOADSP is the default value if you omit both ADSP and NOADSP.

AUDITOR | NOAUDITOR

AUDITOR
specifies that the new user will have full responsibility for auditing the use of system resources, and will be able to control the logging of detected accesses to any RACF-protected resources during RACF authorization checking and accesses to the RACF data base.

You must have the SPECIAL attribute to enter the AUDITOR operand.

NOAUDITOR
specifies that the new user will not have the AUDITOR attribute. NOAUDITOR is the default value if you omit both AUDITOR and NOAUDITOR.

AUTHORITY(*group-authority*)
specifies the level of group authority for the new user in the default group. The valid group authority values are USE, CREATE, CONNECT, and JOIN and are described in "Group Authorities" on page 11. If you omit this operand or specify AUTHORITY without *group-authority*, the default value is USE.

This operand is group-related. If a user is connected to other groups (with the CONNECT command), the user can have a different group authority in each group.

CICS
Note: *This operand applies to z/OS systems only and requires CICS/ESA* 3.2.1 or later*.

This operand defines CICS operator information for a new CICS terminal user.

You can control access to an entire CICS segment or to individual fields within the CICS segment by using field level access checking. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

OPCLASS(*operator-class1*,*operator-class2*,...)
specifies numbers in the range of 1 through 24 representing classes assigned to this operator to which BMS (basic mapping support) messages will be routed.

OPIDENT(*operator-id*)
specifies a 1-to-3-character identification of the operator for use by BMS.

Operator identifiers may consist of any characters, and may be entered with or without single quotation marks. The following rules hold:

- If parentheses, commas, blanks, or semicolons are to be entered as part of the operator identifier, the character string must be enclosed in single quotation marks. For example, if the operator identifier is `(1)`, you must enter `OPIDENT('(1)')`.
- If a single quotation mark is intended to be part of the operator identifier, and the entire character string is enclosed in single quotation marks, two single quotation marks must be entered together for each single quotation mark within the string. For example, if the operator identifier is `1',` (a one, followed by a single quotation mark, followed by a comma), then you would enter `OPIDENT('1'',')`. Note that the whole string must be within single quotation marks due to the presence of the comma.
- If the first character of the operator identifier is a single quotation mark, then the string must be entered within single quotation marks and two single quotation marks entered for the first character. For example, if the operator identifier is `'12` (a quote followed by a one, followed by a two), you would enter `OPIDENT(''12')`.

OPPRTY(*operator-priority*)
specifies the number in the range of 0 through 255 that represents the priority of the operator.

TIMEOUT(*timeout-value*)
specifies the time in minutes that the operator is allowed to be idle before being signed off. If specified, TIMEOUT must be a number in the range of 0 through 60. TIMEOUT defaults to 0 if omitted, meaning no timeout.

XRFSOFF(FORCE | NOFORCE)
FORCE means that the user will be signed off by CICS when an XRF takeover occurs.

CLAUTH | NOCLAUTH

CLAUTH(*class-name* ...)
specifies the classes in which the new user is allowed to define profiles to RACF for protection. Classes you can specify are USER, and any resource classes defined in the class descriptor table.

To enter the CLAUTH operand, you must have the SPECIAL attribute or have the CLAUTH attribute for the classes specified. If you do not have sufficient authority for a specified class, RACF

ignores the CLAUTH specification for that class and continues processing with the next class name specified.

Note: The CLAUTH attribute has no meaning for the FILE and DIRECTRY classes.

NOCLAUTH
specifies that the new user is not to have the CLAUTH attribute. NOCLAUTH is the default if you omit both CLAUTH and NOCLAUTH.

DATA('*installation-defined-data*')
specifies up to 255 characters of installation-defined data to be stored in the user's profile. It may also contain double-byte character set (DBCS) data and must be enclosed in single quotation marks. Note that only 254 characters are chained off the ACEE.

Use the LISTUSER command to list this information.

The data is available (in a user's ACEE) to RACROUTE REQUEST=DEFINE and RACROUTE REQUEST=AUTH for preprocessing and postprocessing installation exit routines, and to RACROUTE REQUEST=VERIFY for postprocessing installation exit routines.

DFLTGRP(*group-name*)
specifies the name of a RACF-defined group to be used as the default group for the user. If you do not specify a group, RACF uses your current connect group as the default.

Note: You do not have to issue the CONNECT command to connect new users to their default groups.

DFP
Note: *This operand applies to z/OS systems only.*

specifies that, when you define a user to RACF, you can enter any of the following suboperands to specify default values for DFP data application identifier, data class, management class, and storage class. DFP uses this information to determine data management and DASD storage characteristics when a user creates a new data set.

You can control access to an entire DFP segment or to individual fields within the DFP segment by using field level access checking. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

DATAAPPL(*application-name*)
specifies an 8-character DFP data application identifier.

DATACLAS(*data-class-name*)
specifies the default data class. The maximum length of *data-class-name* is 8 characters.

A data class can specify some or all of the physical data set attributes associated with a new data set. During new data set allocation, data management uses the value you specify as a default unless it is preempted by a higher priority default, or overridden in some other way, for example by JCL.

Note: The value you specify must be a valid data class name defined for use on your system. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

For information on defining DFP data classes, see *MVS/Extended Architecture Storage Administration Reference*.

MGMTCLAS(*management-class-name*)
specifies the default management class. The maximum length of *management-class-name* is 8 characters.

A management class contains a collection of management policies that apply to data sets. Data management uses the value you specify as a default unless it is preempted by a higher priority default, or overridden in some other way, for example by JCL.

Note: The value you specify must be protected by a profile in the MGMTCLAS general resource class, and the user must be granted at least READ access to the profile. Otherwise, RACF does not allow the user access to the specified MGMTCLAS. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

For information on defining DFP management classes, see *MVS/Extended Architecture Storage Administration Reference*.

STORCLAS(*storage-class-name*)
specifies the default storage class. The maximum length of *storage-class-name* is 8 characters.

A storage class specifies the service level (performance and availability) for data sets managed by the storage management subsystem (SMS). During new data set allocation, data management uses the value you specify as a default unless it is preempted by a higher priority default, or overridden in some other way (for example, by JCL).

Note: The value you specify must be protected by a profile in the STORCLAS general resource class, and the user must be granted at least READ access to the profile. Otherwise, RACF will not allow the user access to the specified STORCLAS. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

For information on defining DFP storage classes, see *MVS/Extended Architecture Storage Administration Reference*.

GRPACC | NOGRPACC
Note: *These operands apply to z/OS systems only.*

GRPACC
specifies that any group data sets protected by DATASET profiles defined by the new user will be automatically accessible to other users in the group. The group whose name is used as the high-level qualifier of the data set name (or the qualifier supplied by a command installation exit) will have UPDATE access authority in the new profile. GRPACC specified on the ADDUSER command overrides NOGRPACC specified on the CONNECT command.

NOGRPACC
specifies that the new user will not have the GRPACC attribute. NOGRPACC is the default value if you omit both GRPACC and NOGRPACC.

LANGUAGE
Note: *This operand applies to z/OS systems only.*

specifies the user's preferred national languages. Specify this operand if the user is to have languages other than the system-wide defaults (established by the LANGUAGE operand on the SETROPTS command).

For the primary and secondary languages, specify either the installation-defined name of a currently active language (a maximum of 24 characters) or one of the language codes (three characters in length) for a language installed on your system.

- If this profile is for a TSO/E user who will establish an extended MCS console session, the languages you specify should be one of the languages specified on the LANGUAGE LANGCODE statements in the MMSLSTxx PARMLIB member. See your z/OS system programmer for this information.

  For more information on TSO/E national language support, see *TSO/E Customization*.
- If this profile is for a CICS user, see your CICS administrator for the languages supported by CICS on your system.

  For more information, see *CICS-RACF Security Guide*.

PRIMARY(*language*)
specifies the user's primary language.

The language name can be a quoted or unquoted string; *language* must be either the installation-defined name of a currently active language (a maximum of 24 characters), or one of the language codes (three characters in length) for a language installed on your system.

SECONDARY(*language*)
specifies the user's secondary language.

The language name can be a quoted or unquoted string; *language* must be either the installation-defined name of a currently active language (a maximum of 24 characters), or one of the language codes (three characters in length) for a language installed on your system.

Note:

1. The same language can be specified for with both PRIMARY and SECONDARY parameters.
2. If RACF is not running under MVS/ESA SP 4.1 or later, or if the z/OS message service is not active, or if it is running under z/VM, the PRIMARY and SECONDARY values must be a 3-character language code.

MFA[PWFALLBACK | NOPWFALLBACK]) | NOMFA
enables or disables MFA for the new user. Note that a protected user is created only when the new user has no password, no passphrase, and is not enabled for MFA.

PWFALLBACK
specifies the new user is allowed to use the FALLBACK command parameter on the z/VM LOGON command. FALLBACK enables the traditional RACF authentication methods (password, passphrase,etc.) to be in effect for a valid LOGON FALLBACK request.

NOPWFALLBACK
specifies the new user is not allowed to use the FALLBACK command parameter on the z/VM LOGON command. That is, LOGON via MFA will always be required, and the request will be denied should MFA fail or be unavailable. NOPWFALLBACK is the default when MFA is specified.

NOMFA
disables MFA for the user. This is the default.

MODEL(*dsname*)
Note: *This operand applies to z/OS systems only.*

specifies the name of a discrete data set profile that will be used as a model when new data set profiles are created that have *userid* as the high-level qualifier. For this operand to be effective, the MODEL(USER) option (specified on the SETROPTS command) must be active.

RACF always prefixes the data set name with *userid* when it accesses the model. For information about automatic profile modeling, refer to *z/VM: RACF Security Server Security Administrator's Guide*.

NAME('*user-name*')
specifies the user name to be associated with the new user ID. You can use a maximum of any 20 characters. If the name you specify contains any blanks, it must be enclosed in single quotation marks.

If you omit the NAME operand, RACF uses a default of 20 # (X'7B') characters ('###...'). Note, however, that the corresponding entry in a LISTUSER output will be the word “unknown”.

OPERATIONS | NOOPERATIONS

OPERATIONS
on z/OS, specifies that the new user will have authorization to do maintenance operations on all RACF-protected data sets, tape volumes, and DASD volumes except those where the access list specifically limits the OPERATIONS user to a lower access authority than the operation requires.

On z/VM, the OPERATIONS attribute allows the user to access z/VM resources except those where the resource's access list specifically limits the OPERATIONS user to a lower access authority.

You establish the lower access authority for the OPERATIONS user through the PERMIT command. OPERATIONS specified on ADDUSER overrides NOOPERATIONS specified on the CONNECT command.

You must have the SPECIAL attribute to enter the OPERATIONS operand.

NOOPERATIONS
specifies that the new user is not to have the OPERATIONS attribute. NOOPERATIONS is the default if you omit both OPERATIONS and NOOPERATIONS.

OPERPARM

Note: *These operands apply to z/OS systems only.*

specifies default information used when this user establishes an extended MCS console session.

You can control access to the entire OPERPARM segment or to individual fields within the OPERPARM segment by using field level access checking. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

For information on planning how to use OPERPARM segments, see *MVS/ESA Planning: Operations*.

Note:

1. You need not specify every suboperand in an OPERPARM segment. In general, if you omit a suboperand, the default is the same as the default in the CONSOLxx PARMLIB member, which can also be used to define consoles.
2. If you specify MSCOPE or ROUTCODE but do not specify a value for them, RACF uses MSCOPE(*ALL) and ROUTCODE(NONE) to update the corresponding fields in the user profile, and these values will appear in listings of the OPERPARM segment of the user profile.
3. If you omit the other suboperands, RACF does not update the corresponding fields in the user's profile, and no value will appear in listings of the OPERPARM segment of the profile.

ALTGRP(*alternate-console-group*)
specifies the console group used in recovery. It can be 1 to 8 characters in length, with valid characters being 0 through 9, A through Z, # (X'7B'), $ (X'5B'), or @ (X'7C').

AUTH(MASTER | ALL | INFO | any others)
specifies the authority this console has to issue operator commands.

If you omit this operand, RACF will not add this field to the user's profile. However, an extended MCS console will use AUTH(INFO) when a session is established.

MASTER
allows this console to act as a master console, which can issue all z/OS operator commands.

ALL
allows this console to issue system control commands, input/output commands, console control commands, and informational commands.

INFO
allows this console to issue informational commands.

CONS
allows this console to issue console control and informational commands.

IO
allows this console to issue input/output and informational commands.

SYS
allows this console to issue system control commands and informational commands.

AUTO(YES | NO)
specifies whether the extended console can receive messages that have been automated by the Message Processing Facility (MPF) in the sysplex.

If you omit this operand, RACF does not add this field to the user's profile. However, an extended MCS console will use AUTO(NO) when a session is established.

CMDSYS(*system-name* | *)
specifies the system to which commands issued from this console are to be sent. *System-name* must be 1 to 8 characters, with valid characters being A through Z, 0 through 9, and @ (X'7C'), # (X'7B'), $ (X'5B'). If * is specified, commands are processed on the local system where the console is attached.

If you omit this operand, RACF does not add this field to the user's profile. However, an extended MCS console will use CMDSYS(*) when a session is established.

DOM(NORMAL | ALL | NONE)
specifies whether this console receives delete operator message (DOM) requests.

If you omit this operand, RACF does not add this field to the user's profile. However, an extended MCS console will use DOM(NORMAL) when a session is established.

NORMAL
specifies that the system queues all appropriate DOM requests to this console.

ALL
specifies that all systems in the sysplex queue DOM requests to this console.

NONE
specifies that no DOM requests are queued to this console.

KEY(*searching-key*)
specifies a 1 to 8 byte character name that can be used to display information for all consoles with the specified key by using the z/OS command, DISPLAY CONSOLES,KEY. If specified, KEY can include A through Z, 0 through 9, # (X'7B'), $ (X'5B'), or @ (X'7C').

If you omit this operand, RACF does not add this field to the user's profile. However, an extended MCS console will use a KEY value of NONE when a session is established.

LEVEL(*message-level*)
specifies the messages that this console is to receive. Can be a list of R, I, CE, E, IN, NB or ALL. If you specify ALL, you cannot specify R, I, CE, E, or IN.

If you omit this operand, RACF does not add this field to the user's profile. However, an extended MCS console will use LEVEL(ALL) when a session is established.

NB
specifies that the console receives *no* broadcast messages.

ALL
specifies that the console receives all of the following messages (R, I, CE, E, IN).

R
specifies that the console receives messages requiring an operator reply.

I
specifies that the console receives immediate action messages.

CE
specifies that the console receives critical eventual action messages.

E
specifies that the console receives eventual action messages.

IN
specifies that the console receives informational messages.

LOGCMDRESP(SYSTEM | NO)
specifies if command responses are to be logged.

If you omit this operand, RACF does not add this field to the user's profile. However, an extended MCS console will use LOGCMDRESP(SYSTEM) when a session is established.

SYSTEM
specifies that command responses are logged in the hardcopy log.

NO
specifies that command responses are not logged.

MFORM(*message-format*)
specifies the format in which messages are displayed at the console. Can be a combination of T, S, J, M, and X:

J
Messages are displayed with a job ID or name.

M
Message text is displayed.

S
Messages are displayed with the name of the originating system.

T
Messages are displayed with a time stamp.

X
Messages that are flagged as exempt from job name and system name formatting are ignored.

If you omit this operand, RACF will not add this field to the user's profile. However, an extended MCS console will use MFORM(M) when a session is established.

MIGID(YES | NO)
specifies that a 1-byte migration ID is to be assigned to this console. The migration ID allows command processors that use a 1-byte console ID to direct command responses to this console.

If you omit this operand, RACF does not add this field to the user's profile. However, an extended MCS console will use MIGID(NO) when a session is established.

MONITOR(*events*)
specifies which information should be displayed when jobs, TSO sessions, or data set status are being monitored.

If you omit this operand, RACF does not add this field to the user's profile. However, an extended MCS console will use MONITOR(JOBNAMES SESS) when a session is established. *events* can be a list of the following:

JOBNAMES | JOBNAMEST
displays information about the start and end of each job. JOBNAMES omits the times of job start and job end. JOBNAMEST displays the times of job start and job end.

SESS | SESST
displays information about the start and end of each TSO session. SESS omits the times of session start and session end. SESST displays them.

STATUS
specifies that the information displayed when a data set is freed or unallocated should include the data set status.

MSCOPE(*system-names* | * | *ALL)
specifies the systems from which this console can receive messages that are not directed to a specific console.

If you omit this operand, RACF does not add this field to the user's profile. However, an extended MCS console will use MSCOPE(*ALL) when a session is established.

If you specify MSCOPE but omit a value, RACF will use MSCOPE(*ALL) to update this field in the user's profile. *ALL will appear in listings of the OPERPARM segment of the user's profile.

system-names
is a list of one or more system names, where *system-name* can be any combination of A through Z, 0 through 9, # (X'7B'), $ (X'5B'), or @ (X'7C').

*
is the system on which the console is currently active.

***ALL**
All systems.

ROUTCODE(ALL | NONE | *routing-codes*)
specifies the routing codes of messages this console is to receive.

If you omit this operand, RACF does not add this field to the user's profile. However, an extended MCS console will use ROUTCODE(NONE) when a session is established.

If you specify ROUTCODE but omit a value, RACF uses ROUTCODE(NONE) to update this field in the user's profile. NONE will appear in listings of the OPERPARM segment of the user's profile. The value for ROUTCODE can be one of the following:

ALL
All routing codes.

NONE
No routing codes.

routing-codes
One or more routing codes or sequences of routing codes. The routing codes can be list of n and n1:n2, where n, n1, and n2 are integers from 1 to 128, and n2 is greater than n1.

STORAGE(*amount*)
specifies the amount of storage in megabytes in the TSO/E user's address space that can be used for message queuing to this console. If specified, STORAGE must be a number between 1 and 2000.

If you omit this operand, RACF does not add this field to the user's profile. However, an extended MCS console will use STORAGE(1) when a session is established and a value of 0 will be listed in the OPERPARM segment of the user's profile to indicate that no storage value was specified.

UD(YES | NO)
specifies whether this console is to receive undelivered messages.

If you omit this operand, RACF does not add this field to the user's profile. However, an extended MCS console will use UD(NO) when a session is established.

OVM
specifies OpenExtensions information for the user being defined to RACF. Each suboperand defines information that RACF stores in a field in the OVM segment of the user's profile.

You can control access to an entire OVM segment or to individual fields in the OVM segment by using field-level access checking.

FSROOT(*file-system-root*)
specifies the pathname for the file system root.

When you define the FSROOT pathname to RACF, it can be from 1 to 1023 characters. The FSROOT pathname can consist of any characters and can be entered with or without single quotation marks. The following rules apply:

- If parentheses, commas, blanks, or semicolons are to be entered as part of the pathname, the character string must be enclosed in single quotation marks.
- If a single quotation mark is intended to be part of the pathname and the entire character string is enclosed in single quotation marks, two single quotation marks must be entered together for each single quotation mark within the string.
- If the first character of the pathname is a single quotation mark, then the string must be entered within single quotation marks and two single quotation marks entered for the first character.

Both uppercase and lowercase are accepted and maintained in the case in which they are entered. The fully-qualified pathname should be specified. RACF does not ensure that a valid pathname has been specified.

If FSROOT is not specified, z/VM sets the file system root for the user to the value specified in the CP directory. If no value is specified in the CP directory, the user has to issue the OPENVM MOUNT command to mount the appropriate file system.

The z/VM command line will not allow you to enter a pathname as long as 1023 characters. See “RAC (Enter RACF Commands on z/VM)” on page 207 for instructions on entering a long RACF command.

HOME(*initial-directory-name*)
specifies the user's OpenExtensions initial directory pathname. The initial directory is part of the file system. This will be the current working directory.

When you define a HOME pathname to RACF, it can be from 1 to 1023 characters. The HOME pathname can consist of any characters and can be entered with or without single quotation marks. The following rules apply:

- If parentheses, commas, blanks, or semicolons are to be entered as part of the pathname, the character string must be enclosed in single quotation marks.
- If a single quotation mark is intended to be part of the pathname and the entire character string is enclosed in single quotation marks, two single quotation marks must be entered together for each single quotation mark within the string.
- If the first character of the pathname is a single quotation mark, then the string must be entered within single quotation marks and two single quotation marks entered for the first character.

Both uppercase and lowercase are accepted and maintained in the case in which they are entered. The fully-qualified pathname should be specified. RACF does not ensure that a valid pathname has been specified.

If HOME is not specified, z/VM sets the working directory for the user to the value specified in the CP directory. If no value is specified in the CP directory, z/VM sets the working directory for the user to "/" (the root directory).

The z/VM command line will not allow you to enter a pathname as long as 1023 characters. See "RAC (Enter RACF Commands on z/VM)" on page 207 for instructions on entering a long RACF command.

PROGRAM(*program-name*)
specifies the PROGRAM pathname (shell program). This will be the first program started when the OPENVM SHELL command is entered.

When you define a PROGRAM pathname to RACF, it can be from 1 to 1023 characters. The PROGRAM pathname can consist of any characters and can be entered with or without single quotation marks. The following rules apply:

- If parentheses, commas, blanks, or semicolons are to be entered as part of the pathname, the character string must be enclosed in single quotation marks.
- If a single quotation mark is intended to be part of the pathname and the entire character string is enclosed in single quotation marks, two single quotation marks must be entered together for each single quotation mark within the string.
- If the first character of the pathname is a single quotation mark, then the string must be entered within single quotation marks and two single quotation marks entered for the first character.

Both uppercase and lowercase are accepted and maintained in the case in which they are entered. The fully-qualified pathname should be specified. RACF does not ensure that a valid pathname has been specified.

If PROGRAM is not specified, z/VM sets the PROGRAM pathname to the value specified in the CP directory. If no value is specified in the CP directory, z/VM gives control to the default shell program (/bin/sh) when the OPENVM SHELL command is issued.

The z/VM command line will not allow you to enter a pathname as long as 1023 characters. See "RAC (Enter RACF Commands on z/VM)" on page 207 for instructions on entering a long RACF command.

UID(*user-identifier*)
specifies the user identifier. The UID is a numeric value between 0 and 2 147 483 647.

Be careful about assigning 0 as the user identifier. A UID of 0 is considered a superuser. The superuser will pass all OpenExtensions security checks.

If the UID is not specified, the user will be assigned the default UID of 4 294 967 295 (X'FFFFFFFF'). The LISTUSER command displays the field name followed by the word “NONE”.

Note: RACF does not require the UID to be unique. The same value can be assigned to multiple users but this is not recommended because individual user control would be lost. However, if you want a set of users to have exactly the same access to the OpenExtensions resources, you may decide to assign the same UID to more than one user.

OWNER(*userid* or *group-name*)
specifies a RACF-defined user or group to be assigned as the owner of the RACF profile for the user being added. If you omit this operand, you are defined as the owner.

PASSWORD | NOPASSWORD

PASSWORD(*password*)
specifies the user's initial logon password. This password is always set expired, thus forcing the user to change the password at initial logon. Note that the password syntax rules your installation defines using SETROPTS PASSWORD do not apply to this password.

NOPASSWORD
specifies that the new user does not have a password which can be used to authenticate the user. This allows you the option of defining a user which can only authenticate by using a password phrase and/or MFA, which are generally both stronger than a password.

Specifying a user as a NOPASSWORD user can also be used as an extra safeguard for service machine user IDs which are not meant to be logged on to directly. When a user has no password, no password phrase, and is not enabled for MFA, the user is a protected user. If a protected user attempts to enter the system with a password, with a password phrase, or with MFA, the attempt fails. However, the user ID is not revoked due to the failed password attempts even if the SETROPTS PASSWORD(REVOKE) option is in effect.

The ability to define a "phrase-only" user and/or "MFA-only" user depends on whether the user uses any applications which check passwords, and which do not support password phrases or MFA. See the descriptions of the MFA operand above and the PHRASE operand below.

Note:

1. Protected user IDs can only enter the system by means of an AUTOLOG or XAUTOLOG command, and are protected from being revoked through inactivity or unsuccessful attempts to access the system using incorrect passwords, password phrases, and MFA credentials. The PROTECTED attribute will appear in LISTUSER output for any such user. See *z/VM: RACF Security Server Security Administrator's Guide* for more information.
2. The NOPASSWORD attribute will appear in LISTUSER output for any user without a password but with a password phrase.
3. The PASSDATE field will be displayed as "N/A" for any user without a password.
4. Specifying NOPASSWORD will suppress the ICH01022I message which is issued by ADDUSER if neither PASSWORD nor NOPASSWORD is specified.

PHRASE(*'password phrase'*)
Specifies the user's initial password phrase. The password phrase you define is a text string of up to 100 characters and must be enclosed in single quotation marks. By default, the password phrase must be at least 14 characters long, but can be as short as 9 characters if the new-password-phrase exit (ICHPWX11) allows it. The password phrase is always set expired, thus requiring the user to change it on initial use.

The following syntax rules apply to all password phrases. You cannot alter these syntax rules. You cannot add additional rules of your own unless your installation tailors the new-password-phrase exit (ICHPWX11). For programming details, see *z/VM: RACF Security Server System Programmer's Guide*.

Password Phrase Syntax Rules

- Must not contain the user ID (as sequential uppercase or sequential lowercase characters)
- Must contain at least 2 alphabetic characters (A-Z, a-z)

- Must contain at least 2 non-alphabetic characters (numerics, punctuation, or special characters)
- Must not contain more than 2 consecutive characters that are identical
- Must be enclosed in single quotation marks, with single quotation marks within the password phrase doubled
- Must not contain forward slashes, nulls (X'00'), or leading or trailing blanks

If ICHPWX11 is present, it can reject the specified password phrase. Password phrases shorter than 14 characters will be rejected by RACF unless ICHPWX11 is present and allows the new value.

If the specified password phrase is accepted, it is made the user's current password phrase and, when SETROPTS PASSWORD(HISTORY) is in effect, it is added to the user's password phrase history.

If you omit PHRASE, no password phrase is assigned. If you enter PHRASE without a *password phrase* value, you are prompted for a value if you are in a RACF command session.

The PASSPHRASE attribute will appear in LISTUSER output for any user who has been assigned a password phrase.

ROAUDIT | NOROAUDIT

ROAUDIT
Specifies that the new user has full responsibility for auditing the use of system resources.

You must have the SPECIAL attribute to enter the ROAUDIT operand.

NOROAUDIT
Specifies that the new user does not have the ROAUDIT attribute.

SECLABEL(*security-label*)
specifies the user's default security label, where *security-label* is an installation-defined security label name that represents an association between a particular security level and zero or more security categories.

If the user does not enter a security label when logging on, this value becomes the user's current security label.

A security label corresponds to a particular security level (such as CONFIDENTIAL) with a set of zero or more security categories (such as PAYROLL or PERSONNEL).

For a list of security labels that you can use, enter:

```
SEARCH CLASS(SECLABEL)
```

When the SECLABEL class is not active, RACF ignores this operand. When no member of the SECLABEL profile exists for *security-label*, you are prompted to provide a valid *security-label*.

SECLEVEL(*security-level*)
specifies the user's security level, where *security-level* is an installation-defined security level name that must be a member of the SECLEVEL profile in the SECDATA class. The *security-level* that you specify corresponds to the number of the minimum security level that a user must have to access the resource.

When you specify SECLEVEL and the SECDATA class is active, RACF adds security level access checking to its other authorization checking. If global access checking does not grant access, RACF compares the security level allowed in the user profile with the security level required in the resource profile. If the security level in the user profile is less than the security level in the resource profile, RACF denies the access. If the security level in the user profile is equal to or greater than the security level in the resource profile, RACF continues with other authorization checking.

Note: RACF does not perform security level checking for a started procedure with the privileged attribute.

When the SECDATA class is not active, RACF ignores this operand. When no member of the SECLEVEL profile exists for *security-level*, you are prompted to provide a valid *security-level*.

SPECIAL | NOSPECIAL

SPECIAL
specifies that the new user will be allowed to issue all RACF commands with all operands except the operands that require the AUDITOR attribute. SPECIAL specified on the ADDUSER command overrides NOSPECIAL specified on the CONNECT command.

You must have the SPECIAL attribute to enter the SPECIAL operand.

NOSPECIAL
specifies that the new user is not to have the SPECIAL attribute. NOSPECIAL is the default if you omit both SPECIAL and NOSPECIAL.

TSO
Note: *This operand applies to z/OS systems only.*

specifies that, when you define a TSO user to RACF, you can enter any of the following suboperands to specify default TSO logon information for that user. Each suboperand defines information that RACF stores in a field within the TSO segment of the user's profile.

You can control access to an entire TSO segment or to individual fields within the TSO segment by using field level access checking. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

ACCTNUM(*account-number*)
specifies the user's default TSO account number when logging on through the TSO/E logon panel. The account number you specify must be protected by a profile in the ACCTNUM general resource class, and the user must be granted READ access to the profile. Otherwise, the user cannot log on to TSO using the specified account number.

Account numbers may consist of any characters, and may be entered with or without single quotation marks. The following rules hold:

- If parentheses, commas, blanks, or semicolons are to be entered as part of the account number, the character string must be enclosed in single quotation marks. For example, if the account number is `(123)`, you must enter `ACCTNUM('(123)')`.
- If a single quotation mark is intended to be part of the account number, and the entire character string is enclosed in single quotation marks, two single quotation marks must be entered together for each single quotation mark within the string. For example, if the account number is `1',` (a one, followed by a single quotation mark, followed by a comma), then you would enter `ACCTNUM('1'',')`. Note that the whole string must be within single quotation marks due to the presence of the comma.
- If the first character of the account number is a single quotation mark, then the string must be entered within single quotation marks and two single quotation marks entered for the first character. For example, if the account number is `'12` (a quote followed by a one, followed by a two), you would enter `ACCTNUM(''''12')`.

A user can change an account number, or specify an account number if one has not been specified, using the TSO/E logon panel. RACF checks the user's authorization to the specified account number. If the user is authorized to use the account number, RACF stores the account number in the TSO segment of the user's profile, and TSO/E uses it as a default value the next time the user logs on to TSO/E. Otherwise, RACF denies the use of the account number.

Note that when you define an account number on TSO, you can specify 1 to 40 characters. When you define a TSO account number to RACF, you can specify only 1 to 39 characters.

DEST(*destination-id*)
specifies the default destination to which the user can route dynamically allocated SYSOUT data sets. *destination-id* must be 1 to 7 alphanumeric characters, beginning with an alphabetic or national character.

HOLDCLASS(*hold-class*)
specifies the user's default hold class. The specified value must be 1 alphanumeric character, excluding national characters.

If you specify the TSO operand on the ADDUSER command but do not specify a value for HOLDCLASS, RACF uses a default value consistent with current TSO defaults.

JOBCLASS(*job-class*)
specifies the user's default job class. The specified value must be 1 alphanumeric character, excluding national characters.

If you specify the TSO operand on the ADDUSER command but do not specify a value for JOBCLASS, RACF uses a default value consistent with current TSO defaults.

MAXSIZE(*maximum-region-size*)
specifies the maximum region size the user can request at logon. The *maximum-region-size* is the number of 1024-byte units of virtual storage that TSO can create for the user's private address space. The specified value can be an integer in the range of 0 through 65535 for MVS/370 systems, or an integer in the range of 0 through 2096128 for MVS/XA* or later systems.

If you specify the TSO operand on the ADDUSER command but do not specify a value for MAXSIZE, or specify MAXSIZE(0), RACF uses a default value consistent with current TSO defaults.

Note: This operand is not relevant to z/VM.

MSGCLASS(*message-class*)
specifies the user's default message class. The specified value must be 1 alphanumeric character, excluding national characters.

If you specify the TSO operand on the ADDUSER command but do not specify a value for MSGCLASS, RACF uses a default value consistent with current TSO defaults.

PROC(*logon-procedure-name*)
specifies the name of the user's default logon procedure when logging on through the TSO/E logon panel. The name you specify must be 1 to 8 alphanumeric characters and begin with an alphabetic character. The name must also be defined as a profile in the TSOPROC general resource class, and the user must be granted READ access to the profile. Otherwise, the user cannot log on to TSO using the specified logon procedure.

A user can change a logon procedure, or specify a logon procedure if one has not been specified, using the TSO/E logon panel. RACF checks the user's authorization to the specified logon procedure. If the user is authorized to use the logon procedure, RACF stores the name of the procedure in the TSO segment of the user's profile, and TSO/E uses it as a default value the next time the user logs on to TSO/E. Otherwise, RACF denies the use of the logon procedure.

SECLABEL(*security-label*)
specifies the user's security label if one was entered on the TSO LOGON panel. On subsequent LOGONs, it appears automatically on the panel.

Note: For more information on the relationship between the TSO security label and the user's security label, see *z/VM: RACF Security Server Security Administrator's Guide*.

SIZE(*default-region-size*)
specifies the minimum region size if the user does not request a region size at logon. The default region size is the number of 1024-byte units of virtual storage available in the user's private address space at logon. The specified value can be an integer in the range of 0 through 65535 for MVS/370 systems, or an integer in the range of 0 through 2096128 for MVS/XA or later systems.

A user can change the minimum region size, or specify the minimum region size if one has not been specified, using the TSO/E logon panel. RACF stores this value in the TSO segment of the user's profile and TSO/E uses it as a default value the next time the user logs on to TSO/E.

If you (or a user) specify a value for SIZE that is greater than MAXSIZE, RACF sets SIZE equal to MAXSIZE.

Note: This operand is not relevant to z/VM.

SYSOUTCLASS(*sysout-class*)
specifies the user's default SYSOUT class. The specified value must be 1 alphanumeric character, excluding national characters.

If you specify the TSO operand on the ADDUSER command but do not specify a value for SYSOUTCLASS, RACF uses a default value consistent with current TSO defaults.

UNIT(*unit-name*)
specifies the default name of a device or group of devices that a procedure uses for allocations. The specified value must be 1 to 8 alphanumeric characters.

USERDATA(*user-data*)
specifies optional installation data defined for the user. The specified value must be 4 EBCDIC characters; valid characters are 0 through 9 and A through F.

UACC(*access-authority*)
specifies the default value for the universal access authority for all new resources the user defines while connected to the specified default group. The universal access authorities are ALTER, CONTROL, UPDATE, READ, and NONE. (RACF does not accept EXECUTE access authority with the ADDUSER command.) If you omit this operand or specify UACC without an access authority, the default is NONE.

This operand is group-related. If a user is connected to other groups (with the CONNECT command), the user can have a different default universal access authority in each group.

Note: When an z/OS user (who has the ADSP attribute or specifies the PROTECT parameter on a JCL DD statement) enters the system using his or her default group as the current connect group, RACF assigns this default universal access authority value to any data set or tape volume profiles the user defines.

WHEN([DAYS(*day-info*)][TIME(*time-info*)])
specifies the days of the week and/or the hours in the day when the user is allowed to access the system from a terminal. The day-of-week and time restrictions apply only when a user logs on to the system; that is, RACF does not force the user off the system if the end-time occurs while the user is logged on. Also, the day and time restrictions do not apply to batch jobs; the user can submit a batch job on any day and at any time.

If you omit the WHEN operand, the user can access the system at any time. If you specify the WHEN operand, you can restrict the user's access to the system to certain days of the week or to a certain time period within each day. Otherwise, you can restrict access to both certain days of the week and to a certain time period within each day.

To allow a user to access the system only on certain days, specify DAYS(day-info), where *day-info* can be any one of the following:

ANYDAY
the user can access the system on any day. If you omit DAYS, ANYDAY is the default.

WEEKDAYS
the user can access the system only on weekdays (Monday through Friday).

day ...
the user can access the system only on the days specified, where *day* can be MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, or SUNDAY, and you can specify the days in any order.

To allow a user to access the system only during a certain time period of each day, specify TIME(*time-info*), where *time-info* can be any one of the following:

ANYTIME
specifies that the user can access the system at any time. If you omit TIME, ANYTIME is the default.

start-time*:*end-time
specifies that the user can access the system only during the specified time period. The format of both start-time and end-time is hhmm, where hh is the hour in 24-hour notation (00 through 23) and mm is the minutes (00 through 59). Note that 0000 is not a valid time value.

If start-time is greater than end-time, the interval spans midnight and extends into the following day.

If you omit DAYS and specify TIME, the time restriction applies to all seven days of the week. If you specify both DAYS and TIME, the user can access the system only during the specified time period and only on the specified days.

WORKATTR

Note: *These operands apply to z/OS systems only.*

WAACCNT(*account-number*)
specifies an account number for APPC/MVS processing.

You can specify a maximum of 255 EBCDIC characters. If the value contains any blanks, it must be enclosed in single quotation marks.

WAADDR*n* (*address-line*)
specifies up to four additional address lines for SYSOUT delivery. *n* can be any number from 1 to 4.

For each *address-line*, you can specify a maximum of 60 EBCDIC characters. If an address line contains any blanks, it must be enclosed in single quotation marks.

WABLDG(*building*)
specifies the building that SYSOUT information is to be delivered to.

You can specify a maximum of 60 EBCDIC characters. If the value contains any blanks, it must be enclosed in single quotation marks.

WADEPT(*department*)
specifies the department that SYSOUT information is to be delivered to.

You can specify a maximum of 60 EBCDIC characters. If the value contains any blanks, it must be enclosed in single quotation marks.

WANAME(*name*)
specifies the name of the user that SYSOUT information is to be delivered to.

You can specify a maximum of 60 EBCDIC characters. If the value contains any blanks, it must be enclosed in single quotation marks.

WAROOM(*room*)
specifies the room that SYSOUT information is to be delivered to.

You can specify a maximum of 60 EBCDIC characters. If the value contains any blanks, it must be enclosed in single quotation marks.

Examples

Example 1

Operation	User IA0 wants to define users PAJ5 and ESH25 to RACF and assign RESEARCH as their default group.
Known	User IA0 has JOIN authority to group RESEARCH and the CLAUTH attribute for the USER class. User PAJ5 and ESH25 are not defined to RACF. User IA0 is currently connected to group RESEARCH.
Command	`ADDUSER (PAJ5 ESH25)`
Defaults	NAME(####################) NOPASSWORD OWNER(IA0) DFLTGRP(RESEARCH) AUTHORITY(USE) UACC(NONE) NOGRPACC NOADSP NOSPECIAL NOOPERATIONS NOCLAUTH NOAUDITOR NOROAUDIT

Example 2

Operation: User WJE10 wants to define user RGH01 to RACF and assign PAYROLL as the default and owning group. The password will be PASS, group authority will be CREATE, and universal access authority will be READ.

Known: User WJE10 has JOIN authority to group PAYROLL and the CLAUTH attribute for the USER class.

User WJE10 is not currently connected to group PAYROLL.

User RGH01 is not defined to RACF.

The name of user RGH01 is RG Harris.

Command:
```
ADDUSER RGH01 DFLTGRP(PAYROLL) OWNER(PAYROLL)
PASSWORD(PASS) NAME('R. G. HARRIS')
AUTHORITY(CREATE) UACC(READ)
```

Defaults: NOSPECIAL NOOPERATIONS NOCLAUTH NOAUDITOR NOROAUDIT

Example 3

Operation: User RACFMIN wants to define user PIZ30 to RACF with a security category of NEWEMPLOYEE and a security level of NOSECRETS. User PIZ30 is to be allowed to use the system only on weekdays between the hours of 8:00 A.M. and 6:00 P.M.

Known: User RACFMIN has the SPECIAL attribute. NEWEMPLOYEE has been defined to RACF as a valid category, and NOSECRETS has been defined as a valid security level. The new user's name is John Doe.

Command:
```
ADDUSER PIZ30 NAME('JOHN DOE')
ADDCATEGORY(NEWEMPLOYEE) SECLEVEL(NOSECRETS)
WHEN(DAYS(WEEKDAYS)TIME(0800:1800))
```

Defaults: OWNER(RACFMIN) NOGRPACC NOSPECIAL NOOPERATIONS NOAUDITOR NOADSP AUTHORITY(USE) NOPASSWORD NOROAUDIT

Example 4

Operation: A user with SPECIAL authority wants to define a user that has both a password and a password phrase.

Known: The user's name is Jasper M. Wells. Bruce is the owner of the RACF profile.

Command:
```
ADDUSER JASPERW OWNER(BRUCE) NAME('JASPER M.
WELLS') PASSWORD(W00F) PHRASE('My name is Jasper
& I''m a good boy!')
```

Defaults: NOGRPACC NOSPECIAL NOOPERATIONS NOAUDITOR NOADSP AUTHORITY(USE) NOROAUDIT

Example 5

Operation The user with SPECIAL authority wants to define a "phrase-only" user.

Known The user's name is Stewart Griffin. LOISG is the owner of the RACF profile.

Command
```
ADDUSER STEWIEG OWNER(LOISG) NAME('STEWART
GRIFFIN') PHRASE('I shall rule the world!')
```

Defaults NOGRPACC NOSPECIAL NOOPERATIONS NOAUDITOR NOADSP AUTHORITY(USE) NOPASSWORD NOROAUDIT

ALTDIR (Alter SFS Directory Profile)

System environment

SFS directories apply to z/VM systems only.

Purpose

Use the ALTDIR command to modify an existing RACF profile protecting an SFS directory.

To have changes take effect after altering a generic profile, one of the following steps is required:

- The security administrator issues the SETROPTS command:

```
SETROPTS GENERIC(DIRECTRY) REFRESH
```

- The user of the resource logs off and logs on again

Related Commands

- To protect an SFS directory with a discrete or generic profile, use the ADDDIR command as described in "ADDDIR (Add SFS Directory Profile)" on page 16.
- To delete an SFS directory profile, use the DELDIR command as described in "DELDIR (Delete SFS Directory Profile)" on page 134.
- To list the information in the SFS directory profiles, use the LDIRECT command as described in "LDIRECT (List SFS Directory Profile)" on page 148.
- To permit or deny access to an SFS directory profile, use the PERMDIR command as described in "PERMDIR (Maintain SFS Directory Access Lists)" on page 194.
- To obtain a list of SFS directory profiles, use the SRDIR command as described in "SRDIR (Obtain a List of SFS Directory Profiles)" on page 324.

Authorization Required

To alter the profile for a directory you must have sufficient authority over it. RACF makes the following checks until one of the conditions is met:

- You have the SPECIAL attribute.
- The directory profile is within the scope of a group in which you have the group-SPECIAL attribute.
- You are the owner of the directory profile.
- The userid qualifier of the directory name matches your user ID.
- To assign a security label, you must have the SPECIAL attribute or have READ access to the security label profile. However, the security administrator can limit the ability to assign security labels to only users with the SPECIAL attribute.
- To assign a security category to a profile, you must have the SPECIAL attribute, or the access category must be in your user profile.
- To assign a security level to a profile, you must have the SPECIAL attribute, or, in your own profile, a security level that is equal to or greater than the security level you are assigning.

For discrete profiles only:

- You are on the access list for the directory and you have ALTER authority. If you have any other level of authority, you may not use the command for this directory.

- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is in the access list and has ALTER authority.
- The universal access authority for the directory is ALTER.

For both discrete and generic profiles, when you specify the GLOBALAUDIT operand:

- You have the AUDITOR attribute or the profile is within the scope of a group in which you have group-AUDITOR attribute.

The GLOBALAUDIT operand has restrictions noted with the description.

Syntax

The complete syntax of the ALTDIR command is:

```
ALTDIR              profile-name
                    [ ADDCATEGORY(category-name ...) | DELCATEGORY
                    [(category-name ... | *)] ]
                    [ APPLDATA('application-defined-data') | NOAPPLDATA ]
                    [ AUDIT( access-attempt [(audit-access-level)] ...)]
                    [ DATA('installation-defined-data') | NODATA ]
                    [ GLOBALAUDIT( access-attempt [(audit-access-level)] ...) ]
                    [ LEVEL(nn) ]
                    [ NOTIFY[(userid)] | NONOTIFY ]
                    [ OWNER(userid or group-name) ]
                    [ SECLABEL(security-label) | NOSECLABEL ]
                    [ SECLEVEL(security-level) | NOSECLEVEL ]
                    [ UACC(access-authority) ]
                    [ WARNING | NOWARNING ]
```

Note: This command is an extension of the RALTER command as it applies to the DIRECTRY class. Other RALTER parameters, such as SESSION and TIMEZONE are also accepted on the command, but are not listed here. If they are specified on this command, they will be ignored.

Parameters

profile-name
specifies the name of the discrete or generic profile to be modified on the RACF database. For the format of these profile names, see "Profile Names for SFS Files and Directories" on page 342. You may specify only one profile.

This operand is required and must be the first operand following ALTDIR.

ADDCATEGORY | DELCATEGORY

ADDCATEGORY(*category-name ...*)
specifies one or more names of installation-defined security categories. The *category-name* must be defined as a member of the CATEGORY profile in the SECDATA class. (For information on defining security categories, see *z/VM: RACF Security Server Security Administrator's Guide*.)

Specifying ADDCATEGORY causes RACF to add any category names you specify to any list of required categories that already exists in the resource profile. All users previously allowed to access the resource can continue to do so only if their profiles also include the additional values for category-names.

When the SECDATA class is active and you specify ADDCATEGORY, RACF performs security category checking in addition to its other authorization checking. If a user requests access to a directory, RACF compares the list of security categories in the user's profile with the list of security categories in the directory profile. If RACF finds any security category in the directory profile that is not in the user's profile, RACF denies access to the directory. If the user's profile contains all the required security categories, RACF continues with other authorization checking.

When the SECDATA class is not active, RACF ignores this operand. When the CATEGORY profile does not include a member for a *category-name*, you are prompted to provide a valid *category-name*.

DELCATEGORY[(*category-name* ...|*)]
specifies one or more names of installation-defined security categories you want to delete from the directory profile. Specifying an asterisk (*) deletes all categories; RACF no longer performs security category checking for the directory profile.

Specifying DELCATEGORY by itself causes RACF to delete from the profile only undefined category names (those category names that were once known to RACF but that the installation has since deleted from the CATEGORY profile.)

When the SECDATA class is not active, RACF ignores this operand. When the CATEGORY profile does not include a member for a *category-name*, you are prompted to provide a valid *category-name*.

APPLDATA | NOAPPLDATA

APPLDATA('*application-defined-data*')
specifies a text string that will be associated with the named resource. The text string may contain a maximum of 255 characters and must be enclosed in single quotation marks. It may also contain double-byte character set (DBCS) data.

NOAPPLDATA
specifies that the ALTDIR command is to delete the text string that was present in the profile associated with this directory.

AUDIT(*access-attempt* [(*audit-access-level*)])

(*access-attempt*)
specifies which access attempts you want to log on the SMF data file. The following options are available:

ALL
indicates that you want to log both authorized accesses and detected unauthorized access attempts.

FAILURES
indicates that you want to log detected unauthorized attempts.

NONE
indicates that you do not want any logging to be done.

SUCCESS
indicates that you want to log authorized accesses.

audit-access-level
specifies which access level(s) you want to log on the SMF data file. The levels you can specify are:

ALTER
logs ALTER access-level attempts only.

CONTROL
logs access attempts at the CONTROL and ALTER levels.

READ
logs access attempts at any level. READ is the default value if you omit audit-access-level.

UPDATE
logs access attempts at the UPDATE, CONTROL, and ALTER levels.

DATA | NODATA

DATA('*installation-defined-data*')
specifies up to 255 characters of installation-defined data to be stored in the directory profile. The data must be enclosed in single quotation marks. It may also contain double-byte character set (DBCS) data.

Use the LDIRECT command to list this information.

NODATA
specifies that the ALTDIR command is to delete any installation-defined data in the directory profile.

GLOBALAUDIT(*access-attempt* [(*audit-access-level*)])
specifies which access attempts to log on the SMF data file. The options (ALL, SUCCESS, FAILURES, and NONE) and the audit-access levels are the same as those described under the AUDIT operand.

To use the GLOBALAUDIT operand, you must have the AUDITOR attribute, or the profile must be within the scope of a group in which you have the group-AUDITOR attribute.

Note: Regardless of the value specified in GLOBALAUDIT, RACF always logs all access attempts specified on the AUDIT operand.

LEVEL(*nn*)
specifies a level indicator, where nn is an integer between 0 and 99.

Your installation assigns the meaning of the value.

RACF includes it in all records that log SFS directory accesses and in the LDIRECT command display.

NOTIFY | NONOTIFY

NOTIFY[(*userid*)]
specifies the user ID of a user to be notified whenever RACF uses this profile to deny access to a directory. If you specify NOTIFY without specifying a user ID, RACF takes your user ID as the default; you will be notified whenever the profile denies access to a directory.

A user who is to receive NOTIFY messages should log on frequently to take action in response to the unauthorized access attempt described in each message. RACF sends NOTIFY messages to the specified user ID. If the user ID is logged on, the message immediately appears on the user's screen. If the user ID is not logged on or is disconnected, RACF sends the message to the user in a reader file. The name of this reader file will be the user ID specified on the NOTIFY keyword, and the type will be NOTIFY. (Note that you should not specify the user ID of a virtual machine that always runs disconnected.)

When the directory profile also includes WARNING, RACF might have granted access to the directory to the user identified in the message.

NONOTIFY
specifies that no user is to be notified when RACF uses this profile to deny access to a directory.

OWNER(*userid* or *group-name*)
specifies a RACF-defined user or group to be assigned as the new owner of the directory profile. To change the owner of a directory, you must be the current owner of the directory or have the SPECIAL attribute, or the profile must be within the scope of a group in which you have the group-SPECIAL attribute.

If you specify OWNER(userid), the user you specify as the owner does not automatically have access to the directory. Use the PERMDIR command to add the owner to the access list as desired.

SECLABEL | NOSECLABEL

SECLABEL(*security-label*)
specifies an installation-defined security label for this profile. A security label corresponds to a particular security level (such as CONFIDENTIAL) with a set of zero or more security categories (such as PAYROLL or PERSONNEL).

For a list of security labels that you are authorized to use, enter:

```
SEARCH CLASS(SECLABEL)
```

RACF stores the name of the security label you specify in the directory profile if you are authorized to use that SECLABEL.

If you are not authorized to the SECLABEL or if the name you had specified is not defined as a SECLABEL profile in the SECLABEL class, the directory profile is not updated.

Note: If the SECLABEL class is active and the security label is specified in this profile, any security levels and categories in the profile are ignored.

NOSECLABEL
removes the security label, if one had been specified, from the profile.

SECLEVEL | NOSECLEVEL

SECLEVEL(*security-level*)
specifies the name of an installation-defined security level. This name corresponds to the number that is the minimum security level that a user must have to access the directory. The *security-level* must be a member of the SECLEVEL profile in the SECDATA class.

When you specify SECLEVEL and the SECDATA class is active, RACF adds security level access checking to its other authorization checking. If global access checking does not grant access, RACF compares the security level allowed in the user profile with the security level required in the directory profile. If the security level in the user profile is less than the security level in the directory profile, RACF denies the access. If the security level in the user profile is equal to or greater than the security level in the directory profile, RACF continues with other authorization checking.

If the SECDATA class is not active, RACF stores the name you specify in the directory profile. When the SECDATA class is activated and the name you specified is defined as a SECLEVEL profile, RACF can perform security level access checking for the directory profile. If the name you specify is not defined as a SECLEVEL profile, you are prompted to provide a valid *security-level*.

NOSECLEVEL
specifies that the ALTDIR command is to delete the security level name from the profile. RACF no longer performs security level access checking for the directory.

UACC(*access-authority*)
specifies the universal access authority to be associated with the directory. The universal access authorities are ALTER, CONTROL, UPDATE, READ, and NONE. See "Access Authority for SFS Files and Directories on z/VM" on page 12 for more information.

WARNING | NOWARNING

WARNING
specifies that, even if access authority is insufficient, RACF is to issue a warning message and allow access to the directory. RACF also records the access attempt in the SMF record if logging is specified in the profile.

NOWARNING
specifies that, if access authority is insufficient, RACF is to deny the user access to the resource and not issue a warning message.

Examples

Example

Operation	Change the owner of directory PAYROLL to user GARYLEE
Known	The file pool ID is FP1. The directory was created is currently owned by KLINE.
Command	`ALTDIR FP1:KLINE.PAYROLL OWNER(GARYLEE)`
Defaults	None

ALTDSD (Alter Data Set Profile)

System environment

Data sets apply to z/OS systems only.

Purpose

Use the ALTDSD command to:

- Modify an existing discrete or generic data set profile.

  Changes made to discrete profiles take effect after the ALTDSD command is processed. Changes made to generic profiles do not take effect until one or more of the following steps is taken:

  – The user of the data set issues the LISTDSD command:

  ```
  LISTDSD DA(data-set-protected-by-the-profile) GENERIC
  ```

  Note: Use the data set name, not the profile name.

  – The security administrator issues the SETROPTS command:

  ```
  SETROPTS GENERIC(DATASET) REFRESH
  ```

  See SETROPTS command for authorization requirements.

  – The user of the data set logs off and logs on again.

  For more information, refer to *z/VM: RACF Security Server Security Administrator's Guide*.
- Protect a single volume of either a multivolume tape data set or a multivolume, non-VSAM DASD data set. (At least one volume must already be RACF-protected.)
- Remove RACF-protection from either a single volume of a multivolume tape data set or a single volume of a multivolume, non-VSAM DASD data set. (You cannot delete the last volume from the profile.)

Note: RACF interprets dates with 2 digit years in the following way, YY represents the 2 digit year.

```
IF 70 < YY <= 99 THEN
   The date is interpreted as 19YY
IF 00 <= YY <= 70 THEN
   The date is interpreted as 20YY
```

Related Commands

- To create a data set profile, use the ADDSD command as described in “ADDSD (Add Data Set Profile)” on page 33.
- To delete a data set profile, use the DELDSD command as described in “DELDSD (Delete Data Set Profile)” on page 136.
- To list a data set profile, use the LISTDSD command as described in “LISTDSD (List Data Set Profile)” on page 160.
- To permit or deny access to a data set profile, use the PERMIT command as described in “PERMIT (Maintain Resource Access Lists)” on page 202.

Authorization Required

To use the ALTDSD command, you must have sufficient authority over the profile. RACF makes the following checks until one of these conditions is met:

- You have the SPECIAL attribute.
- The data set profile is within the scope of a group in which you have the group-SPECIAL attribute.
- You are the owner of the profile.
- The high-level qualifier of the profile name (or the qualifier supplied by the RACF naming conventions table or by a command installation exit) is your user ID.
- To assign a security label, you must have the SPECIAL attribute or have READ access to the security label profile. However, the security administrator can limit the ability to assign security labels only to users with the SPECIAL attribute.
- To access the DFP segment, field level access checking is required.

For discrete profiles only, one of the following conditions must be met:

- You are in the access list for the discrete profile and you have ALTER authority. (If you have any other level of authority, you may not alter this profile.)
- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is in the access list and has ALTER authority. (If any group that RACF checked has any other level of authority, you may not alter this profile.)
- The universal access authority is ALTER.

To use the GLOBALAUDIT operand, you must have the AUDITOR attribute, or the data set profile must be within the scope of a group in which you have the group-AUDITOR attribute.

If you have the AUDITOR attribute or the data set profile is within the scope of a group in which you have the group-AUDITOR attribute, but you do not satisfy one of the above checks, you may specify only the GLOBALAUDIT operand.

To assign a security category to a profile, you must have the SPECIAL attribute, or the access category must be in your user profile. To assign a security level to a profile, you must have the SPECIAL attribute, or, in your own profile, a security level that is equal to, or greater than, the security level you are assigning.

Syntax

The complete syntax of the ALTDSD command is:

```
ALTDSD          (profile-name [/password] ...)
ALD             [ ADDCATEGORY(category-name ...)
                  | DELCATEGORY [({category-name ...|*} )] ]
                [ ADDVOL(volume-serial) | DELVOL(volume-serial) ]
                [ ALTVOL(old-volume-serial new-volume-serial) ]
                [ AUDIT( access-attempt [(audit-access-level)] ...) ]
                [ DFP(RESOWNER(userid or group-name)) | NODFP ]
                [ DATA('installation-defined-data') | NODATA ]
                [ ERASE | NOERASE ]
                [ GENERIC | NOSET | SET ]
                [ GLOBALAUDIT( access-attempt [(audit-access-level)] ...) ]
                [ LEVEL(nn) ]
                [ NOTIFY[(userid)] | NONOTIFY ]
                [ OWNER(userid or group-name) ]
                [ RETPD(nnnnn) ]
                [ SECLABEL(seclabel-name) | NOSECLABEL ]
                [ SECLEVEL(seclevel-name) | NOSECLEVEL ]
                [ UACC(access-authority) ]
                [ UNIT(type) ]
                [ VOLUME(volume-serial) ]
                [ WARNING | NOWARNING ]
```

Parameters

profile-name
specifies the name of a discrete or generic data set profile. If you specify more than one profile name, the list of names must be enclosed in parentheses.

This operand is required and must be the first operand following ALTDSD.

Note:

1. Because RACF uses the RACF database and not the system catalog, you cannot use alias data set names.
2. If you specify a generic profile name, RACF ignores these operands:

   ADDVOL | DELVOL
   ALTVOL
   SET | NOSET
   UNIT
   VOLUME

/password
specifies the data set password if you are altering the profile for a password-protected data set. This operand applies only if you are using the ADDVOL and SET operands for a volume of a multivolume password-protected data set. The WRITE level password must then be specified.

If the command is executing in the foreground and you omit the password for a password-protected data set, RACF uses the logon password. You will be prompted if the password you enter or the logon password is incorrect.

If the command is executing in a batch job and you either omit the password for a password-protected data set or supply an incorrect password, the operator is prompted.

You can use this operand only for tape data sets and non-VSAM DASD data sets. If you specify a generic profile, RACF ignores this operand.

ADDCATEGORY | DELCATEGORY

ADDCATEGORY(*category-name* ...)
specifies one or more names of installation-defined security categories. *category-name* must be defined as a member of the CATEGORY profile in the SECDATA class. (For information on defining security categories, see *z/VM: RACF Security Server Security Administrator's Guide*.)

Specifying ADDCATEGORY on the ALTDSD command causes RACF to add any category-names you specify to any list of required categories that already exists in the data set profile. All users previously allowed to access the data set can continue to do so only if their profiles also include the additional *category-names*.

When the SECDATA class is active and you specify ADDCATEGORY, RACF performs security category checking in addition to its other authorization checking. If a user requests access to a data set, RACF compares the list of security categories in the user profile with the list of security categories in the data set profile. If RACF finds any security category in the data set profile that is not in the user's profile, RACF denies access to the data set. If the user's profile contains all the required security categories, RACF continues with other authorization checking.

Note: RACF does not perform security category checking for a started procedure with the privileged attribute.

When the SECDATA class is not active, RACF ignores this operand. When the CATEGORY profile does not include a member for a category name, you are prompted to provide a valid name.

DELCATEGORY[(*category-name* ...|*)]
specifies one or more names of installation-defined security categories you want to delete from the data set profile. Specifying an asterisk (*) deletes all categories; RACF no longer performs security category checking for the data set profile.

Specifying DELCATEGORY by itself causes RACF to delete from the profile only undefined category names (those category names that were once known to RACF but that the installation has since deleted from the CATEGORY profile.)

When the SECDATA class is not active, RACF ignores this operand. When the CATEGORY profile does not include a member for a category name, you are prompted to provide a valid name.

ADDVOL | DELVOL

ADDVOL(*volume-serial*)
specifies that you want to RACF-protect the portion of the data set residing on this volume. At least one other portion of the data set on a different volume must already have been RACF-protected. You can use this operand only for tape data sets and non-VSAM data sets.

The DASD volume must be online unless you also specify NOSET. If it is not online and you omit NOSET, the ALTDSD command processor will, if you have TSO MOUNT authority, request that the volume be mounted.

RACF ignores this operand if you specify a generic profile name.

Note: The maximum number of volume serials for a tape data set with an entry in the TVTOC is 42.

DELVOL(*volume-serial*)
specifies that you want to remove RACF-protection from the portion of the data set residing on this volume. If no other portions of this data set on another volume are RACF-protected, the command terminates. (Use the DELDSD command to delete the profile from RACF.) You can use this operand only for tape data sets and non-VSAM DASD data sets.

The DASD volume must be online unless you also specify NOSET. If it is not online and you omit NOSET, the ALTDSD command processor requests that the volume be mounted.

RACF ignores this operand if you specify a generic profile name.

ALTVOL(*old-volume-serial new-volume-serial*)
specifies that you want to change the volume serial number in the data set profile. You can specify this operand for both VSAM and non-VSAM DASD data sets, but you cannot specify it for tape data sets. If you specify ALTVOL for a tape data set, the command fails.

When you specify ALTVOL, RACF ignores the SET and NOSET operands and modifies the data set profile, but it does not process the RACF indicator.

RACF ignores this operand if you specify a generic profile name.

To specify ALTVOL, you must have the SPECIAL attribute, or the data set profile must be within the scope of a group in which you have the group-SPECIAL attribute, or the high-level qualifier of the data set name (or the qualifier supplied by a command installation exit routine) must be your user ID.

AUDIT
specifies which new access attempts you want to log on the SMF data set. The following options are available:

ALL
indicates that you want to log both authorized accesses and detected unauthorized access attempts.

FAILURES
indicates that you want to log detected unauthorized access attempts.

NONE
indicates that you do not want any logging to be done.

SUCCESS
indicates that you want to log authorized accesses.

If you specify AUDIT without a value, RACF ignores it.

audit-access-level
specifies which access levels you want to log on the SMF data set. The levels you can specify are:

ALTER
logs ALTER access-level attempts only.

CONTROL
logs access attempts at the CONTROL and ALTER levels.

READ
logs access attempts at any level. READ is the default value if you omit audit-access-level.

UPDATE
logs access attempts at the UPDATE, CONTROL, and ALTER levels.

You cannot audit access attempts at the EXECUTE level.

DATA | NODATA

DATA('*installation-defined-data*')
specifies up to 255 characters of installation-defined data to be stored in the data set profile. It may also contain double-byte character set (DBCS) data and must be enclosed in single quotation marks.

Use the LISTDSD command to list this information. The data is also available to the RACHECK preprocessing and postprocessing installation exit routines and is copied, if this is a model profile, to the installation-defined data area for new data set profiles.

NODATA
specifies that the ALTDSD command is to delete any installation-defined data in the data set profile.

DFP | NODFP

DFP
specifies that, for an SMS-managed data set, you can change the following information:

RESOWNER(*userid or group-name*)
specifies the user ID or group name of the actual owner of the data sets protected by the profile specified in *profile-name-1*. The name specified for RESOWNER must be a RACF-defined user or group. (The data set resource owner, or RESOWNER, is distinguished from the OWNER, which represents the user or group that owns the data set profile).

You can control access to the entire DFP segment or to individual fields within the DFP segment by using field level access checking. For more information, see the *z/VM: RACF Security Server Security Administrator's Guide*.

NODFP
specifies that RACF should delete the DFP segment from the dataset profile.

ERASE | NOERASE

ERASE
specifies that, when SETROPTS ERASE(NOSECLEVEL) is active, data management is to physically erase the DASD data set extents at the time the data set is deleted (scratched) or released for reuse. Erasing the data set means overwriting all allocated extents with binary zeros.

This operand is ignored for the following:

- If the data set is not a DASD data set
- If SETROPTS ERASE(ALL) is specified for your installation (user and data set profile definitions are overridden)
- SETROPTS ERASE(SECLEVEL(*security_level*)) is specified for your installation (data sets equal or higher in security level are always erased, while those lower in security level are never erased)

NOERASE
specifies that data management is not to erase the DASD data set when it is deleted (scratched). If your installation has specified ERASE(ALL) on the SETROPTS command, NOERASE

is meaningless. When ERASE(ALL) is in effect, data management erases all DASD data sets when they are deleted.

GENERIC | NOSET | SET

GENERIC
specifies that RACF is to treat the profile name as a generic name, even if it does not contain any generic characters.

NOSET | SET
specifies whether or not the data set is to be RACF-indicated. RACF ignores SET and NOSET if you do not use the ADDVOL or DELVOL operand or specify a generic profile name.

NOSET
specifies that RACF is not to change the RACF indicator for the data set.

The volume indicated in the ADDVOL or DELVOL operand does not have to be online.

To use NOSET, you must have the SPECIAL attribute, or the data set profile must be within the scope of a group in which you have the group-SPECIAL attribute, or the high-level qualifier of the data set name (or the qualifier supplied by a command installation exit) must be your user ID. If you are not authorized, RACF ignores the NOSET and ADDVOL or DELVOL operands.

SET
specifies that:

- The data set on this volume is to be RACF-indicated if you also specify the ADDVOL operand. If the indicator is already on, the command fails.
- The RACF-indicator for the data set on this volume is to be set off if you also specify the DELVOL operand. If the indicator is already off, the command fails.

For a DASD data set, the volume indicated in the ADDVOL or DELVOL operand must be online.

GLOBALAUDIT
specifies which access attempts the user who has the AUDITOR attribute wants to log on the SMF data set. The options (ALL, SUCCESS, FAILURES, and NONE) and the audit-access levels, are the same as those described under the AUDIT operand.

To use the GLOBALAUDIT operand, you must have the AUDITOR attribute, or the profile must be within the scope of a group in which you have the group-AUDITOR attribute.

Note: Regardless of the value specified in GLOBALAUDIT, RACF always logs all access attempts specified on the AUDIT operand.

LEVEL(*nn*)
specifies a new level indicator, where nn is an integer between 0 and 99.

Your installation assigns the meaning of the value. It is not used by the authorization function in RACHECK but is available to the RACHECK postprocessing installation exit routine.

RACF includes it in all records that log data set accesses and in the LISTDSD command display.

NOTIFY | NONOTIFY

NOTIFY[(*userid*)]
specifies the user ID of a user to be notified whenever RACF uses this profile to deny access to a data set. If you specify NOTIFY without specifying a user ID, RACF takes your user ID as the default; you will be notified whenever the profile denies access to a data set.

A user who is to receive NOTIFY messages should log on frequently, both to take action in response to the unauthorized access attempts the messages describe and to clear the messages from the SYS1.BRODCAST data set. (When the profile also includes WARNING, RACF might have granted access to the data set to the user identified in the message.)

NONOTIFY
specifies that no user is to be notified when RACF uses this profile to deny access to a data set.

OWNER(*userid* or *group-name*)
specifies a RACF-defined user or group to be the new owner of the data set profile. If you specify a user ID as the owner of a group data set profile, the specified user must have at least USE authority in the group to which the data set profile belongs.

To change the owner of a profile, you must be the current owner of the profile or have the SPECIAL attribute, or the profile must be within the scope of a group in which you have the group-SPECIAL attribute.

Note: The user specified as the owner does not automatically have access to the data set. Use the PERMIT command to add the owner to the access list as desired.

RETPD(*nnnnn*)
specifies the RACF security retention period for a tape data set. The security retention period is the number of days that must elapse before a tape data set profile expires. (Note that, even though the data set profile expires, RACF-protection for data sets protected by the profile is still in effect. For more information, see the *z/VM: RACF Security Server Security Administrator's Guide*.)

The number you specify must be 1 to 5 digits in the range of 0 through 65533 or, to indicate a data set that never expires, 99999.

Using RETPD to change the RACF security retention period for a data set means that the RACF security retention period and the data set retention period specified by the EXPDT/RETPD parameters on the JCL DD statement will no longer be the same.

When the TAPEVOL class is active, RACF checks the RACF security retention period before it allows a data set to be overwritten. RACF adds the number of days in the retention period to the creation date for the data set. If the result is less than the current date, RACF continues to protect the data set.

When the TAPEVOL class is not active, RACF ignores the RETPD operand.

Specifying this operand for a DASD data set does not cause an error, but it has no meaning because RACF ignores the operand during authorization checking.

SECLABEL | NOSECLABEL

SECLABEL(*seclabel-name*)
specifies an installation-defined security label for this profile. A security label corresponds to a particular security level (such as CONFIDENTIAL) with a set of zero or more security categories (such as PAYROLL or PERSONNEL).

For a list of security labels that you are authorized to use, enter:

```
SEARCH CLASS(SECLABEL)
```

RACF stores the name of the security label you specify in the data set profile if you are authorized to use that SECLABEL.

If you are not authorized to the SECLABEL or if the name you had specified is not defined as a SECLABEL profile in the SECLABEL class, the data set profile is not created.

Note: If the SECLABEL class is active and the security label is specified in this profile, any security levels and categories in the profile are ignored.

NOSECLABEL
removes the security label, if one had been specified, from the profile.

SECLEVEL | NOSECLEVEL

SECLEVEL(*seclevel-name*)
specifies the name of an installation-defined security level. This name corresponds to the number that is the minimum security level that a user must have to access the data set. The *seclevel-name* must be a member of the SECLEVEL profile in the SECDATA class.

When you specify SECLEVEL and the SECDATA class is active, RACF adds security level access checking to its other authorization checking. If global access checking does not grant access, RACF compares the security level allowed in the user profile with the security level required in the

data set profile. If the security level in the user profile is less than the security level in the data set profile, RACF denies the access. If the security level in the user profile is equal to or greater than the security level in the data set profile, RACF continues with other authorization checking.

Note: RACF does not perform security level checking for a started procedure with the privileged attribute.

If the SECDATA class is not active, RACF stores the name you specify in the data set profile. When the SECDATA class is activated and the name you specified is defined as a SECLEVEL profile, RACF can perform security level access checking for the data set profile. If the name you specify is not defined as a SECLEVEL profile and the SECDATA class is active, you are prompted to provide a valid security level name.

NOSECLEVEL
specifies that the ALTDSD command is to delete the security level name from the profile. RACF no longer performs security level access checking for the data set.

UACC(*access-authority*)
specifies the universal access authority to be associated with the data sets. The universal access authorities are ALTER, CONTROL, READ, UPDATE, EXECUTE, and NONE. If you specify CONTROL for a tape data set or a non-VSAM DASD data set, RACF treats the access authority as UPDATE. If you specify EXECUTE for a tape data set or a DASD data set not used as a program library, RACF treats the access authority as NONE.

If you enter UACC without a value, RACF retains the old universal access authority for the data sets.

UNIT(*type*)
specifies the unit type to be added to the data set profile on which a non-VSAM data set resides. You can specify an installation-defined unit name, a generic device type, or a specific device address. RACF ignores this operand if you specify a generic profile name.

VOLUME(*volume-serial*)
specifies the volume on which the tape data set, the non-VSAM DASD data set, or the catalog for the VSAM data set resides.

If you specify VOLUME and *volume-serial* does not appear in the profile for the data set, the command fails. If you omit VOLUME and the data set name appears more than once in the RACF database, the command fails. If you omit VOLUME and the data set name appears only once in the RACF database, no volume serial checking is performed and processing continues.

RACF ignores this operand if you specify a generic profile name.

WARNING | NOWARNING

WARNING
specifies that, even if access authority is insufficient, RACF is to issue a warning message and allow access to the resource. RACF also records the access attempt in the SMF record if logging is specified in the profile.

NOWARNING
specifies that, if access authority is insufficient, RACF is to deny the user access to the resource and not issue a warning message.

Examples

Example 1

Operation: User AEH0 owns data set profile PAYROLL.DEPT2.DATA and wants to assign ownership of the data set to group PAYROLL. Only users with categories of FINANCIAL and PERSONNEL and a security level of PERSONAL are to be able to access the data set.

Known: Data set PAYROLL.DEPT2.DATA is RACF-defined with a discrete profile. FINANCIAL and PERSONNEL are valid categories of access; PERSONAL is a valid security level name.

Command:
```
ALTDSD 'PAYROLL.DEPT2.DATA' OWNER(PAYROLL)
ADDCATEGORY(FINANCIAL PERSONNEL)
SECLEVEL(PERSONAL)
```

Defaults: None

Example 2

Operation: User WRH0 wants to change the universal access authority to NONE for data set RESEARCH.PROJ02.DATA and wants to have all accesses to the data set logged on SMF records. User ADMIN02 is to be notified when RACF uses this profile to deny access to the data set. The data set is to be erased when it is deleted (scratched).

Known: User WRH0 has ALTER access to data set profile RESEARCH.PROJ02.DATA. User WRH0 is logged onto group RESEARCH.

User ADMIN02 is a RACF-defined user.

Data set RESEARCH.PROJ02.DATA is RACF-defined with a generic profile. The SETROPTS ERASE option has been specified for the installation.

Command:
```
ALTDSD 'RESEARCH.PROJ02.DATA' UACC(NONE)
AUDIT(ALL(READ)) GENERIC NOTIFY(ADMIN02) ERASE
```

Defaults: None

Example 3

Operation: User CD0 wants to remove RACF-protection from volume 222222 of the multivolume data set CD0.PROJ2.DATA.

Known: CD0.PROJ2.DATA is a non-VSAM data set that resides on volumes 111111 and 222222 and is defined to RACF with a discrete profile. Volume 222222 is online. User CDO's TSO profile specifies PREFIX (CDO).

Command:
```
ALTDSD PROJ2.DATA DELVOL(222222)
```

Default: SET

Example 4

Operation: User RVD02 wants to have all successful accesses to data set PAYROLL.ACCOUNT on volume SYS003 to be logged to the SMF data set.

Known: User RVD02 has the AUDITOR attribute.

Command:
```
ALTDSD 'PAYROLL.ACCOUNT'
GLOBALAUDIT(SUCCESS(READ)) VOLUME(SYS003)
```

Defaults: None

Example 5

Operation: User SJR1 wants to modify the installation-defined information associated with the tape data set SYSINV.ADMIN.DATA. The RACF security retention period is to be 360 days.

Known: User SJR1 has ALTER authority to the data set profile.

Tape data set protection is active.

Command:
```
ALTDSD 'SYSINV.ADMIN.DATA' DATA('LIST OF REVOKED
RACF USERIDS') RETPD(360)
```

Defaults: None

Example 6

Operation: User ADM1 wants to log all unauthorized access attempts and all successful updates to data sets protected by the generic profile SALES.ABC.*.

Known: User ADM1 has the SPECIAL attribute.

Command:
```
ALTDSD 'SALES.ABC.*' AUDIT (FAILURES(READ)
SUCCESS (UPDATE))
```

Defaults: None

Example 7

Operation: User ADM1 owns the DFP-managed data set RESEARCH.TEST.DATA3 and wants to assign user ADM6 as the data set resource owner.

Known: Data set RESEARCH.TEST.DATA3 is RACF-defined with a discrete profile. User ADM1 has the SPECIAL attribute, and user ADM6 is defined to RACF.

Command:
```
ALTDSD 'RESEARCH.TEST.DATA3' DFP(RESOWNER(ADM6))
```

Defaults: None

ALTFILE (Alter SFS File Profile)

System environment

SFS files apply to z/VM systems only.

Purpose

Use the ALTFILE command to modify existing RACF profiles protecting SFS files.

To have changes take effect after altering a generic profile, one of the following steps is required:

- The security administrator issues the SETROPTS command:

```
SETROPTS GENERIC(FILE) REFRESH
```

- The user of the resource logs off and logs on again

Related Commands

- To protect an SFS file with a discrete or generic profile, use the ADDFILE command as described in "ADDFILE (Add SFS File Profile)" on page 22.
- To delete an SFS file profile, use the DELFILE command as described in "DELFILE (Delete SFS File Profile)" on page 139.
- To list the information in an SFS file profile, use the LFILE command as described in "LFILE (List SFS File Profile)" on page 154.
- To permit or deny access to an SFS file, use the PERMFILE command as described in "PERMFILE (Maintain SFS File Access Lists)" on page 198.
- To obtain a list of SFS file profiles, use the SRFILE command as described in "SRFILE (Obtain a List of SFS File Profiles)" on page 329.

Authorization Required

To alter the profile for an SFS file you must have sufficient authority over it. RACF makes the following checks until one of the conditions is met:

- You have the SPECIAL attribute.
- The file profile is within the scope of a group in which you have the group-SPECIAL attribute.
- You are the owner of the file profile.
- The user ID qualifier of the file name matches your user ID.
- To assign a security label, you must have the SPECIAL attribute or have READ access to the security label profile. However, the security administrator can limit the ability to assign security labels to only users with the SPECIAL attribute.
- To assign a security category to a profile, you must have the SPECIAL attribute, or the access category must be in your user profile.
- To assign a security level to a profile, you must have the SPECIAL attribute, or, in your own profile, a security level that is equal to or greater than the security level you are assigning.

For discrete profiles only:

- You are on the access list for the file and you have ALTER authority. If you have any other level of authority, you may not use the command for this file.
- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is in the access list and has ALTER authority.

- The universal access authority for the file is ALTER.

For both discrete and generic profiles, when you specify the GLOBALAUDIT operand:

- You have the AUDITOR attribute or the profile is within the scope of a group in which you have group-AUDITOR attribute.

The GLOBALAUDIT operand has restrictions noted with the description.

Syntax

The complete syntax of the ALTFILE command is:

```
ALTFILE              profile-name
ALF                  [ ADDCATEGORY(category-name ...)
                       | DELCATEGORY [({category-name ... | * })] ]
                     [ APPLDATA('application-defined-data') | NOAPPLDATA ]
                     [ AUDIT( access-attempt [(audit-access-level)] ...) ]
                     [ DATA('installation-defined-data') | NODATA ]
                     [ GLOBALAUDIT( access-attempt [(audit-access-level)] ...) ]
                     [ LEVEL(nn) ]
                     [ NOTIFY[(userid)] | NONOTIFY ]
                     [ OWNER(userid or group-name) ]
                     [ SECLABEL(seclabel-name) | NOSECLABEL ]
                     [ SECLEVEL(seclevel-name) | NOSECLEVEL ]
                     [ UACC(access-authority) ]
                     [ WARNING | NOWARNING ]
```

Note: This command is an extension of the RALTER command as it applies to the FILE class. Other RALTER parameters, such as SESSION and TIMEZONE are also accepted on the command, but are not listed here. If they are specified on this command, they will be ignored.

Parameters

profile-name
specifies the name of the discrete or generic profile to be modified in the RACF database. You may specify only one profile. For the format of these profile names, see "Profile Names for SFS Files and Directories" on page 342.

This operand is required and must be the first operand following ALTFILE.

Note: Do not specify a generic character unless SETROPTS GENERIC (or SETROPTS GENCMD) is in effect.

ADDCATEGORY | DELCATEGORY

ADDCATEGORY(*category-name ...*)
specifies one or more names of installation-defined security categories. The *category-name* must be defined as a member of the CATEGORY profile in the SECDATA class. (For information on defining security categories, see *z/VM: RACF Security Server Security Administrator's Guide*.)

Specifying ADDCATEGORY causes RACF to add any category names you specify to any list of required categories that already exists in the resource profile. All users previously allowed to access the resource can continue to do so only if their profiles also include the additional values for category-names.

When SECDATA class is active and you specify ADDCATEGORY, RACF performs security category checking in addition to its other authorization checking. If a user requests access to a file, RACF compares the list of security categories in the user's profile with the list of security categories in the file profile. If RACF finds any security category in the file profile that is not in the user's profile, RACF denies access to the file. If the user's profile contains all the required security categories, RACF continues with other authorization checking.

When the SECDATA class is not active, RACF ignores this operand. When the CATEGORY profile does not include a member for a *category-name*, you are prompted to provide a valid *category-name*.

DELCATEGORY[(*category-name* ...|*)]
specifies one or more names of installation-defined security categories you want to delete from the file profile. Specifying an asterisk (*) deletes all categories; RACF no longer performs security category checking for the file profile.

Specifying DELCATEGORY by itself causes RACF to delete from the profile only undefined category names (those category names that were once known to RACF but that the installation has since deleted from the CATEGORY profile.)

When the SECDATA class is not active, RACF ignores this operand. When the CATEGORY profile does not include a member for a *category-name*, you are prompted to provide a valid *category-name*.

APPLDATA | NOAPPLDATA

APPLDATA('*application-defined-data*')
specifies a text string that will be associated with the named resource. The text string may contain a maximum of 255 characters and must be enclosed in single quotation marks. It may also contain double-byte character set (DBCS) data.

NOAPPLDATA
specifies that the ALTFILE command is to delete the text string that was present in the profile associated with this resource.

AUDIT(*access-attempt* [(*audit-access-level*)])

(*access-attempt*)
specifies which access attempts you want to log on the SMF data file. The following options are available:

ALL
indicates that you want to log both authorized accesses and detected unauthorized access attempts.

FAILURES
indicates that you want to log detected unauthorized attempts.

NONE
indicates that you do not want any logging to be done.

SUCCESS
indicates that you want to log authorized accesses.

audit-access-level
specifies which access level(s) you want logged on the SMF data file. The levels you can specify are:

ALTER
logs ALTER access-level attempts only.

CONTROL
logs access attempts at the CONTROL and ALTER levels.

READ
logs access attempts at any level. READ is the default value if you omit audit-access-level.

UPDATE
logs access attempts at the UPDATE, CONTROL, and ALTER levels.

DATA | NODATA

DATA('*installation-defined-data*')
specifies up to 255 characters of installation-defined data to be stored in the file profile. The data must be enclosed in single quotation marks. It may also contain double-byte character set (DBCS) data.

Use the LFILE command to list this information.

NODATA
specifies that the ALTFILE command is to delete any installation-defined data in the file profile.

GLOBALAUDIT(*access-attempt* [(*audit-access-level*)])
specifies which access attempts the user who has the AUDITOR attribute wants to log on the SMF data file. The options (ALL, SUCCESS, FAILURES, and NONE) and the audit-access levels, are the same as those described under the AUDIT operand.

To use the GLOBALAUDIT operand, you must have the AUDITOR attribute, or the profile must be within the scope of a group in which you have the group-AUDITOR attribute.

Note: Regardless of the value specified in GLOBALAUDIT, RACF always logs all access attempts specified on the AUDIT operand.

LEVEL(*nn*)
specifies a level indicator, where nn is an integer between 0 and 99.

Your installation assigns the meaning of the value.

RACF includes it in all records that log SFS file accesses and in the LFILE command display.

NOTIFY | NONOTIFY

NOTIFY[(*userid*)]
specifies the user ID of a user to be notified whenever RACF uses this profile to deny access to a file. If you specify NOTIFY without specifying a user ID, RACF takes your user ID as the default; you will be notified whenever the profile denies access to a file.

A user who is to receive NOTIFY messages should log on frequently to take action in response to the unauthorized access attempt described in each message. RACF sends NOTIFY messages as follows to the specified user ID. If the user ID is logged on, the message immediately appears on the user's screen. If the user ID is not logged on or is disconnected, RACF sends the message to the user in a reader file. The name of this reader file will be the user ID specified on the NOTIFY keyword, and the type will be NOTIFY. (Note that you should not specify the user ID of a virtual machine that always runs disconnected.)

When the file profile also includes WARNING, RACF might have granted access to the file to the user identified in the message.

NONOTIFY
specifies that no user is to be notified when RACF uses this profile to deny access to a file.

OWNER(*userid* or *group-name*)
specifies a RACF-defined user or group to be assigned as the new owner of the file profile. To change the owner of a file, you must be the current owner of the file or have the SPECIAL attribute, or the profile must be within the scope of a group in which you have the group-SPECIAL attribute.

If you specify OWNER(userid), the user you specify as the owner does not automatically have access to the file. Use the PERMFILE command to add the owner to the access list as desired.

SECLABEL | NOSECLABEL

SECLABEL(*seclabel-name*)
specifies an installation-defined security label for this profile. A security label corresponds to a particular security level (such as CONFIDENTIAL) with a set of zero or more security categories (such as PAYROLL or PERSONNEL).

For a list of security labels that you are authorized to use, enter:

```
SEARCH CLASS(SECLABEL)
```

RACF stores the name of the security label you specify in the file profile if you are authorized to use that SECLABEL.

If you are not authorized to the SECLABEL or if the name you had specified is not defined as a SECLABEL profile in the SECLABEL class, the file profile is not updated.

Note: If the SECLABEL class is active and the security label is specified in this profile, any security levels and categories in the profile are ignored.

NOSECLABEL
removes the security label, if one had been specified, from the profile.

SECLEVEL | NOSECLEVEL

SECLEVEL(*seclevel-name*)
specifies the name of an installation-defined security level. This name corresponds to the number that is the minimum security level that a user must have to access the file. The *seclevel-name* must be a member of the SECLEVEL profile in the SECDATA class.

When you specify SECLEVEL and the SECDATA class is active, RACF adds security level access checking to its other authorization checking. If global access checking does not grant access, RACF compares the security level allowed in the user profile with the security level required in the file profile. If the security level in the user profile is less than the security level in the file profile, RACF denies the access. If the security level in the user profile is equal to or greater than the security level in the file profile, RACF continues with other authorization checking.

If the SECDATA class is not active, RACF stores the name you specify in the file profile. When the SECDATA class is activated and the name you specified is defined as a SECLEVEL profile, RACF can perform security level access checking for the file profile. If the name you specify is not defined as a SECLEVEL profile, you are prompted to provide a valid *seclevel-name*.

NOSECLEVEL
specifies that the ALTFILE command is to delete the security level name from the profile. RACF no longer performs security level access checking for the file.

UACC(*access-authority*)
specifies the universal access authority to be associated with the file. The universal access authorities are ALTER, CONTROL, UPDATE, READ, and NONE. See "Access Authority for SFS Files and Directories on z/VM" on page 12 for more information.

WARNING | NOWARNING

WARNING
specifies that, even if access authority is insufficient, RACF is to issue a warning message and allow access to the file. RACF also records the access attempt in the SMF record if logging is specified in the profile.

NOWARNING
specifies that, if access authority is insufficient, RACF is to deny the user access to the resource and not issue a warning message.

Examples

Example

Operation	User SUSIEB wants user GARYLEE notified whenever an unauthorized person tries to access file REPORT SCRIPT in directory PAYROLL.
Known	The file pool ID is FP1.
Command	`ALTFILE REPORT SCRIPT FP1:SUSIEB.PAYROLL NOTIFY(GARYLEE)`
Defaults	None

ALTGROUP (Alter Group Profile)

System environment

This command applies to both z/OS and z/VM systems.

Purpose

Use the ALTGROUP command to change:

- The superior group of a group
- The owner of a group
- The terminal indicator for a group
- A model profile name for a group
- The installation-defined data associated with a group
- The default segment information for a group (for example, DFP or OVM)

Related Commands

- To create a group profile, use the ADDGROUP command as described in "ADDGROUP (Add Group Profile)" on page 28.
- To delete a group profile, use the DELGROUP command as described in "DELGROUP (Delete Group Profile)" on page 141.
- To connect a user to a group, use the CONNECT command as described in "CONNECT (Connect User to Group)" on page 128.
- To list information for a group profile, use the LISTGRP command as described in "LISTGRP (List Group Profile)" on page 172.
- To remove a user from a group, use the REMOVE command as described on page "REMOVE (Remove User from Group)" on page 246.

Authorization Required

To change the superior group of a group, you must meet at least one of the following conditions:

- You must have the SPECIAL attribute.
- All the following group profiles must be within the scope of a group in which you have the group-SPECIAL attribute:
  - The group whose superior group you are changing
  - The current superior group
  - The new superior group
- You must be the owner of–or have JOIN authority in–both the current and the new superior groups.

Note: You can have JOIN authority in one group and be the owner of or have the group-SPECIAL attribute in the other group.

If you have any of the following, you can specify any operand:

- The SPECIAL attribute
- The group profile is within the scope of a group in which you have the group-SPECIAL attribute
- You are the current owner of the group.

To add, delete, or alter segments such as DFP or OVM in a group's profile:

- You must have the SPECIAL attribute.
- Your installation must permit you to do so via field level access checking.

Syntax

The following operands used with the ALTGROUP command apply to z/OS systems only:

- DFP | NODFP
- MODEL | NOMODEL

The complete syntax of the command is:

```
ALTGROUP          (group-name ...)
ALG               [ DATA('installation-defined-data') | NODATA ]
                  [ OVM(
                    [ GID(group-identifier) | NOGID ]
                    )
                  | NOOVM ]
                  [ OWNER(userid or group-name) ]
                  [ SUPGROUP(group-name) ]
                  [ TERMUACC | NOTERMUACC ]

z/OS Specific
Operands:         [ DFP(
                    [ DATAAPPL(application-name) | NODATAAPPL ]
                    [ DATACLAS(data-class-name) | NODATACLAS ]
                    [ MGMTCLAS(management-class-name) | NOMGMTCLAS ]
                    [ STORCLAS(storage-class-name) | NOSTORCLAS ]
                    )
                  | NODFP ]
                  [ MODEL(dsname) | NOMODEL ]
```

Parameters

group-name
specifies the name of the group whose definition you want to change. If you specify more than one group name, the list of names must be enclosed in parentheses.

This operand is required and must be the first operand following ALTGROUP.

DATA | NODATA

DATA('*installation-defined-data*')
specifies up to 255 characters of installation-defined data to be stored in the group profile. It may also contain double-byte character set (DBCS) data and must be enclosed in single quotation marks.

Use the LISTGRP command to list this information.

NODATA
specifies that the ALTGROUP command is to delete any installation-defined data in the group profile.

DFP | NODFP

Note: *These operands apply to z/OS systems only.*

DFP
specifies that when you change the profile of a group, you can enter any of the following suboperands to add, change, or delete default values for the DFP data application, data class, management class, and storage class. DFP uses this information to determine data management and DASD storage characteristics when a user creates a new data set for a group.

DATAAPPL | NODATAAPPL

DATAAPPL(*application-name*)
specifies the name of a DFP data application. The name you specify can contain up to 8 alphanumeric characters.

NODATAAPPL
specifies that you want to delete the DFP data application name from the DFP segment of the group's profile.

DATACLAS | NODATACLAS

DATACLAS(*data-class-name*)
specifies the default data class. The class name you specify can contain up to 8 alphanumeric characters.

A data class can specify some or all of the physical data set attributes associated with a new data set. During new data set allocation, data management uses the value you specify as a default unless it is preempted by a higher priority default, or overridden in some other way (for example, by JCL).

Note: The value you specify must be a valid data class name defined for use on your system. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

For information on defining DFP data classes, see *MVS/Extended Architecture Storage Administration Reference*.

NODATACLAS
specifies that you want to delete the default data class name from the DFP segment of the group's profile.

MGMTCLAS | NOMGMTCLAS

MGMTCLAS(*management-class-name*)
specifies the default management class. The class name you specify can contain up to 8 alphanumeric characters.

A management class contains a collection of management policies that apply to data sets. Data management uses the value you specify as a default unless it is preempted by a higher priority default, or overridden in some other way (for example, by JCL).

Note: The value you specify must be defined as a profile in the MGMTCLAS general resource class, and the group must be granted at least READ access to the profile. Otherwise, RACF does not allow the group access to the specified MGMTCLAS. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

For information on defining DFP management classes, see *MVS/Extended Architecture Storage Administration Reference*.

NOMGMTCLAS
specifies that you want to delete the default management class name from the DFP segment of the group's profile.

STORCLAS | NOSTORCLAS

STORCLAS(*storage-class-name*)
specifies the default storage class. The class name you specify can contain up to 8 alphanumeric characters.

A storage class specifies the service level (performance and availability) for data sets managed by the Storage Management Subsystem (SMS). During new data set allocation, data management uses the value you specify as a default unless it is preempted by a higher priority default, or overridden in some other way (for example, by JCL).

Note: The value you specify must be defined as a profile in the STORCLAS general resource class, and the group must be granted at least READ access to the profile.

Otherwise, RACF does not allow the group access to the specified STORCLAS. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

For information on defining DFP storage classes, see *MVS/Extended Architecture Storage Administration Reference*.

NOSTORCLAS
specifies that you want to delete the default storage class name from the DFP segment of the group's profile.

NODFP
specifies that RACF should delete the DFP segment from the group's profile.

MODEL | NOMODEL
Note: *These operands apply to z/OS systems only.*

MODEL(*dsname*)
specifies the name of a data set profile that RACF is to use as a model when new data set profiles are created that have *group-name* as the high-level qualifier. For this operand to be effective, the MODEL(GROUP) option on the SETROPTS command must be active. If the ALTGROUP command cannot find the *dsname* profile, it issues a warning message and places the profile name in the group entry.

RACF always prefixes *dsname* with the group name when it accesses the profile.

For information about automatic profile modeling, refer to *z/VM: RACF Security Server Security Administrator's Guide*.

NOMODEL
specifies that the ALTGROUP command is to delete the model name in the group profile.

OVM | NOOVM

OVM
specifies OpenExtensions information for the group profile being changed.

GID | NOGID

GID(*group-identifier*)
specifies the group identifier. The GID is a numeric value between 0 and 2 147 483 647.

Note:

1. RACF does not require the GID to be unique. The same value can be assigned to multiple groups, but this is not recommended because individual group control would be lost. However, if you want a set of groups to have exactly the same access to the OpenExtensions resources, you may decide to assign the same GID to more than one group.
2. Be careful when changing the GID for a group. The following situations may occur.
   - If the file system contains files that contain the old GID as the file owner GID, the members of the group will lose access to those files, depending on the permission bits associated with the file.
   - If files already exist with an owner GID equal to the group's new GID value, the members of the group will gain access to these files.
   - If another group is subsequently given the old value as its GID, the members of this group will have access to the old group's files.
   - If you have an EXEC.G*gid* profile in the VMPOSIX class for the old GID value, make sure you delete this profile and create another to reflect the new value. For an explanation of these profiles, see *z/VM: RACF Security Server Security Administrator's Guide*.

3. RACF allows you to define and connect a user to more than NGROUPS_MAX groups, but when a process is created or OpenExtensions group information is requested, only up to the first NGROUPS_MAX OpenExtensions groups will be associated with the process or user.

   The first NGROUPS_MAX OpenExtensions groups to which a user is connected, in alphabetical order, are the groups that get associated with the OpenExtensions user.

   See *z/VM: RACF Security Server Macros and Interfaces* for information on NGROUPS_MAX in the ICHNGMAX macro.

NOGID
specifies that you want to delete the group identifier from the OVM segment of the group's profile.

If NOGID is specified for the group, the default GID of 4 294 967 295 (X'FFFFFFFF') is assigned. The LISTGRP command displays the field name followed by the word “NONE”.

NOOVM
specifies that RACF is to delete the OVM segment from the group's profile.

OWNER(*userid or group-name*)
specifies a RACF-defined user or group you want to be the new owner of the group.

To change the owner of a group, you must be the current owner of the group, or have the SPECIAL attribute, or have the group-SPECIAL attribute in the group owning the profile.

If you specify a group name, then OWNER and SUPGROUP must specify the same group name.

SUPGROUP(*group-name*)
specifies the name of the RACF-defined group you want to make the new superior group for the group profile you are changing.

The new superior group must not be the same as the current one, and it must not have any level of subgroup relationship to the group you are changing.

To change a superior group, you must have the SPECIAL attribute, the group profile must be within the scope of a group in which you have the group-SPECIAL attribute, or you must have JOIN authority in or, be the owner of, both the current and new superior groups. Note that you can have JOIN authority in one group and be the owner of or have the group-SPECIAL attribute in the other group.

If owner is a group name, OWNER and SUPGROUP must specify the same group name.

TERMUACC | NOTERMUACC

TERMUACC
specifies that, during terminal authorization checking, RACF is to allow the use of the universal access authority for a terminal when it checks whether a user in the group is authorized to access a terminal.

NOTERMUACC
specifies that the group or a user connected to the group must be authorized (using the PERMIT command with at least READ authority) to access a terminal.

Examples

ALTGROUP Examples for Both z/OS and z/VM:

Example 1

Operation: User WJB10 wants to change the superior group and owning group for PROJECTA from RESEARCH to PAYROLL. Users connected to group PROJECTA will be authorized access to terminals according to the universal access authority of the terminal.

Known: User WJB10 has JOIN authority in RESEARCH and is the owner of PAYROLL.

PROJECTA is a subgroup of RESEARCH.

Command:
```
ALTGROUP PROJECTA SUPGROUP(PAYROLL)
OWNER(PAYROLL) TERMUACC
```

Defaults: None

Example 2

Operation: User ADM1 wants to change the superior group for PROJECTB from SYS1 to RESEARCH and assign RESEARCH as the new owner.

Known: User ADM1 has the SPECIAL attribute.

PROJECTB is a subgroup of SYS1.

Command:
```
ALTGROUP PROJECTB SUPGROUP(RESEARCH)
OWNER(RESEARCH)
```

Defaults: None

ALTGROUP Examples for z/OS Only:

Example 3

Operation: User SJR2 wants to change the installation-defined information associated with the RSC1 group and delete the model name.

Known: User SJR2 is the owner of group RSC1.

Command:
```
ALTGROUP RSC1 DATA('RESOURCE USAGE
ADMINISTRATION') NOMODEL
```

Defaults: None

Example 4

Operation User BILLC wants to make the following changes to the profile for group PROJECT6:

- Change the default DFP management class to MCLASS7
- Change the default DFP storage class to SCLASS3
- Change the default DFP data class to DCLASS15
- Delete the default DFP data application.

Known
- User BILLC has the SPECIAL attribute.
- Group PROJECT6 has been defined to RACF, and PROJECT6's group profile contains a DFP segment.
- MCLASS7 has been defined to RACF as a profile in the MGMTCLAS general resource class, and group PROJECT6 has been given READ access to this profile.
- SCLASS3 has been defined to RACF as a profile in the STORCLAS general resource class, and group PROJECT6 has been given READ access to this profile.

Command
```
ALTGROUP PROJECT6 DFP(MGMTCLAS(MCLASS7)
STORCLAS(SCLASS3) DATACLAS(DCLASS15)
NODATAAPPL))
```

Defaults None

ALTUSER (Alter User Profile)

System environment

This command applies to both z/OS and z/VM systems.

Purpose

Use the ALTUSER command to change the information in a user's profile, including the user's system-wide attributes and access authorities. The user profile consists of a RACF segment and, optionally, other segments such as a TSO segment or a DFP segment. You can use this command to change information in any segment of the user's profile.

When you change a user's level of authority in a group (using the AUTHORITY operand), RACF updates the appropriate group profile.For all other changes, RACF changes the user's profile.

Notes:

1. If the user is currently in the system, changes to the attributes (except for OWNER and AUTHORITY) do not take effect until the next time the user enters the system, although the LISTUSER command shows the new values.
2. RACF interprets dates with 2 digit years in the following way, YY represents the 2 digit year.

```
IF 70 < YY <= 99 THEN
   The date is interpreted as 19YY
IF 00 <= YY <= 70 THEN
   The date is interpreted as 20YY
```

Related Commands

- To add a user profile, use the ADDUSER command as described in “ADDUSER (Add User Profile)” on page 45.
- To delete a user profile, use the DELUSER command as described in “DELUSER (Delete User Profile)” on page 143.
- To display information from a user profile, use the LISTUSER command as described in “LISTUSER (List User Profile)” on page 179.
- To enter a command containing a long pathname, use the RAC command as described in “RAC (Enter RACF Commands on z/VM)” on page 207.

Authorization Required

The level of authority required depends on which of the user's attributes you want to change.

- If you have the SPECIAL attribute, you can use all the operands except UAUDIT/NOUAUDIT.
- If the owner of the user profile is within the scope of a group in which you have the group-SPECIAL attribute, you can use all of the operands except SPECIAL, AUDITOR, ROAUDIT, OPERATIONS, UAUDIT/NOUAUDIT, and NOEXPIRED.
- If you are the owner of the user's profile, you can use any of the following operands for user-related attributes:

ADSP | NOADSP	GRPACC | NOGRPACC	PASSWORD | NOPASSWORD
DATA | NODATA	MODEL | NOMODEL	RESUME | NORESUME
DFLTGRP	NAME	REVOKE | NOREVOKE
EXPIRED	OWNER	WHEN

- Each user can change his or her name field or default group (NAME and DFLTGRP operands). Each user can also change his or her model data set profile name (using the MODEL operand).
- You can use the GROUP, AUTHORITY, and UACC operands for group-related user attributes if you have JOIN or CONNECT authority, or if the group profile is within the scope of a group in which you have the group-SPECIAL attribute, or if you are the owner of the specified group.
- To specify the AUDITOR/NOAUDITOR, ROAUDIT/NOROAUDIT, SPECIAL/NOSPECIAL, and OPERATIONS/NOOPERATIONS operands as system-wide user attributes, you must have the SPECIAL attribute.
- To specify the UAUDIT/NOUAUDIT operand, either you must have the AUDITOR attribute, or the user profile must be within the scope of a group in which you have the group-AUDITOR attribute.
- You can specify the CLAUTH and NOCLAUTH operands, if you are the owner of the user's profile and have the CLAUTH attribute for the class to be added or deleted.
- To assign a security category to a profile, or to delete a category from a profile, you must have the SPECIAL attribute, or the category must be in your user profile.
- To assign a security level to a profile, or to delete a security level from a profile, you must have the SPECIAL attribute, or, in your own profile, a security level that is equal to or greater than the security level you are assigning or deleting.
- To assign a security label to a profile, or to delete a security label from a profile, you must have the SPECIAL attribute, or, in your own profile, a security label that is equal to or greater than the security label you are assigning or deleting. However, the security administrator can limit the ability to assign or delete security labels to only users with the SPECIAL attribute.
- To define information within a segment other than the RACF segment (such as the TSO, DFP, or other segments), you must have one of the following:
  - The SPECIAL attribute
  - At least UPDATE authority to the desired field within the segment via field level access control.
- To reset passwords and password phrases or to resume user IDs, you must have at least one of the following authorizations:
  - You have the SPECIAL attribute.
  - You have group-SPECIAL authority over the user profile.
  - You are the OWNER of the user profile.
  - You have sufficient access to the IRR.PASSWORD.RESET resource in the FACILITY class.
  - You have sufficient access to an appropriate resource in the FACILITY class (IRR.PWRESET.OWNER.*owner* or IRR.PWRESET.TREE.*owner*), and *both* of the following conditions are also true:
    - The other user does not have the SPECIAL, OPERATIONS, AUDITOR, PROTECTED, or ROAUDIT attribute.
    - You are not excluded from altering the user by the IRR.PWRESET.EXCLUDE. *excluded-user* resource in the FACILITY class.

  For more information about the IRR.PWRESET profiles, see *z/VM: RACF Security Server Security Administrator's Guide*.

  When your reset and resume authority is through your access to the IRR.PASSWORD.RESET resource, the IRR.PWRESET.OWNER.*owner* resource, or the IRR.PWRESET.TREE.*owner* resource, the following requirements apply:

  - If you have READ access, you can:
    - Use the PASSWORD operand to reset a password (to an expired password) for a user who does not have the SPECIAL, OPERATIONS, AUDITOR, PROTECTED, or ROAUDIT attribute.
    - Use the PHRASE operand to reset a password phrase (to an expired password phrase) for a user with an assigned password phrase who does not have the SPECIAL, OPERATIONS, AUDITOR, PROTECTED, or ROAUDIT attribute.

Note: You cannot use the PHRASE operand to *add* a password phrase for a user who does not have one.

- Use the RESUME operand, without specifying a date, for a user who does not have the SPECIAL, OPERATIONS, AUDITOR, or PROTECTED attribute.

– If you have UPDATE access, you can:

- Use the PASSWORD, PHRASE, and RESUME operands as noted for READ access.
- Use the NOEXPIRED operand (with PASSWORD or PHRASE) for a user who does not have the SPECIAL, OPERATIONS, AUDITOR, PROTECTED, or ROAUDIT attribute.

– If you have CONTROL access, you can:

- Use the PASSWORD, PHRASE, RESUME, and NOEXPIRED operands as noted for READ and UPDATE access.
- Reset the password or password phrase within the minimum change interval for a user who does not have the SPECIAL, OPERATIONS, AUDITOR, PROTECTED, or ROAUDIT attribute.

- You can use the MFA and NOMFA operands if:
  – You have the SPECIAL or GROUP SPECIAL attribute
  – The owner of the user profile is within the scope of a group in which you have the group-SPECIAL attribute
  – You are the owner of the user's profile

Syntax

The following operands used with the ALTUSER command apply to z/OS systems only:

- ADSP | NOADSP
- CICS | NOCICS
- DFP | NODFP
- GRPACC | NOGRPACC
- LANGUAGE | NOLANGUAGE
- MODEL | NOMODEL
- OPERPARM | NOOPERPARM
- TSO | NOTSO
- WORKATTR | NOWORKATTR

The complete syntax of the command is:

```
ALTUSER          (userid ...)
ALU              [ ADDCATEGORY(category-name ...)
                 | DELCATEGORY[(category-name ...|*)] ]
                 [ AUDITOR | NOAUDITOR ]
                 [ AUTHORITY(group-authority) ]
                 [ {CLAUTH | NOCLAUTH} (class-name ...) ]
                 [ DATA('installation-defined-data') | NODATA ]
                 [ DFLTGRP(group-name) ]
                 [ EXPIRED | NOEXPIRED ]
                 [ GROUP(group-name) ]
                 [ MFA([ PWFALLBACK | NOPWFALLBACK ] ) | NOMFA ]
                 [ NAME('user-name') ]
                 [ OPERATIONS | NOOPERATIONS ]
                 [ OVM(
                   [ FSROOT(file-system-root) |  NOFSROOT ]
                   [ HOME(initial-directory-name) | NOHOME ]
                   [ PROGRAM(program-name) | NOPROGRAM ]
                   [ UID(user-identifier) | NOUID ]
                   )
                 | NOOVM ]
                 [ OWNER(userid or group-name) ]
                 [ PASSWORD (password) | NOPASSWORD ]
                 [ PHRASE ('password phrase') | NOPHRASE ]
                 [ PWCLEAN ]
                 [ PWCONVERT ]
                 [ RESUME [(date)]  | NORESUME ]
                 [ REVOKE [(date)]  | NOREVOKE ]
                 [ ROAUDIT | NOROAUDIT ]
                 [ SECLABEL(seclabel-name) | NOSECLABEL ]
                 [ SECLEVEL(seclevel-name) | NOSECLEVEL]
                 [ SPECIAL | NOSPECIAL ]
                 [ UACC(access-authority) ]
                 [ UAUDIT | NOUAUDIT ]
                 [ WHEN( [DAYS(day-info)] [TIME(time-info)] ) ]
```

z/OS Specific Operands:

[ADSP | NOADSP]
[CICS(
  [OPCLASS(*operator-class1,operator-class2,...*)
    | NOOPCLASS]
  [OPIDENT(*operator-id*) | NOOPIDENT]
  [OPPRTY(*operator-priority*) | NOOPPRTY]
  [TIMEOUT(*timeout-value*) | NOTIMEOUT]
  [XRFSOFF(FORCE | NOFORCE) | NOXRFSOFF]
)
| NOCICS]
[DFP(
  [DATAAPPL(*application-name*) | NODATAAPPL]
  [DATACLAS(*data-class-name*) | NODATACLAS]
  [MGMTCLAS(*management-class-name*) | NOMGMTCLAS]
  [STORCLAS(*storage-class-name*) | NOSTORCLAS]
)
| NODFP]
[GRPACC | NOGRPACC]
[LANGUAGE(
  [PRIMARY(*language*) | NOPRIMARY]
  [SECONDARY(*language*) | NOSECONDARY]
)
| NOLANGUAGE]
[MODEL(*dsname*) | NOMODEL]

```
[ OPERPARM(
  [ ALTGRP(alternate-console-group) | NOALTGROUP  ]
  [ AUTH(operator-authority) | NOAUTH ]
  [ AUTO( YES | NO ) | NOAUTO ]
  [ CMDSYS(system-name) | NOCMDSYS ]
  [ DOM( NORMAL | ALL | NONE ) | NODOM ]
  [ KEY(searching-key) | NOKEY ]
  [ LEVEL(message-level) | NOLEVEL ]
  [ LOGCMDRESP( SYSTEM | NO ) | NOLOGCMDRESP ]
  [ MFORM(message-format) | NOMFORM ]
  [ MIGID( YES | NO ) | NOMIGID ]
  [ MONITOR(event) | NOMONITOR ]
  [ MSCOPE( system-names | * | *ALL ) | NOMSCOPE ]
  [ ROUTCODE( ALL | NONE | routing-codes )
    | NOROUTCODE ]
  [ STORAGE(amount) | NOSTORAGE ]
  [ UD( YES | NO ) | NOUD ]
  )
| NOOPERPARM ]
[ TSO (
  [ ACCTNUM(account-number) | NOACCTNUM ]
  [ DEST(destination-id) | NODEST ]
  [ HOLDCLASS(hold-class) | NOHOLDCLASS ]
  [ JOBCLASS(job-class) | NOJOBCLASS ]
  [ MAXSIZE(maximum-region-size) | NOMAXSIZE ]
  [ MSGCLASS(message-class) | NOMSGCLASS ]
  [ PROC(logon-procedure-name) | NOPROC ]
  [ SECLABEL(seclabel-name) | NOSECLABEL ]
  [ SIZE(default-region-size) | NOSIZE ]
  [ SYSOUTCLASS(sysout-class) | NOSYSOUTCLASS ]
  [ UNIT(unit-name) | NOUNIT ]
  [ USERDATA(user-data) | NOUSERDATA ]
  )
| NOTSO ]
[ WORKATTR(
  [ WAACCNT(account-number) | NOWAACCNT ]
  [ WAADDR1(address-line-1) | NOWADDR1 ]
  [ WAADDR2(address-line-2) | NOWADDR2 ]
  [ WAADDR3(address-line-3) | NOWADDR3 ]
  [ WAADDR4(address-line-4) | NOWADDR4 ]
  [ WABLDG(building) | NOWABLDG ]
  [ WADEPT(department) | NOWADEPT ]
  [ WANAME(name) | NOWANAME ]
  [ WAROOM(room) | NOWAROOM ]
  )
| NOWORKATTR ]
```

Parameters

userid

specifies the RACF-defined user or users whose profile you want to change. If you specify more than one user ID, the list must be enclosed in parentheses.

This operand is required and must be the first operand following ALTUSER.

ADDCATEGORY | DELCATEGORY

ADDCATEGORY(*category-name*)
specifies one or more names of installation-defined security categories. The names you specify must be defined as members of the CATEGORY profile in the SECDATA class. (For information on defining security categories, see *z/VM: RACF Security Server Security Administrator's Guide*.)

When the SECDATA class is active and you specify ADDCATEGORY, RACF performs security category checking in addition to its other authorization checking. If a user requests access to a data set, RACF compares the list of security categories in the user profile with the list of security categories in the data set profile. If RACF finds any security category in the data set profile that is not in the user's profile, RACF denies access to the data set. If the user's profile contains all the required security categories, RACF continues with other authorization checking.

Note: RACF does not perform security category checking for a started procedure with the privileged or trusted attribute.

When the SECDATA class is not active, RACF ignores this operand. When the CATEGORY profile does not include a member for *category-name*, you are prompted to provide a valid category name.

DELCATEGORY[(*category-name...*|*)]
specifies one or more names of the installation-defined security categories you want to delete from the user profile. Specifying an asterisk (*) deletes all categories; the user no longer has access to any resources protected by security category checking.

Specifying DELCATEGORY without *category-name* causes RACF to delete only undefined category names (those names that once were valid names but that the installation has since deleted from the CATEGORY profile.)

When the SECDATA class is not active, RACF ignores this operand. When the CATEGORY profile does not include a member for a *category-name*, you are prompted to provide a valid *category-name*.

ADSP | NOADSP
Note: *These operands apply to z/OS systems only.*

ADSP
assigns the ADSP attribute to the user. This means that all permanent tape and DASD data sets the user creates will automatically be RACF-protected by discrete profiles. ADSP specified on the ALTUSER command overrides NOADSP specified on the CONNECT command.

The ADSP attribute has no effect (even if assigned to a user) if SETROPTS NOADSP is in effect.

NOADSP
specifies that the user no longer has the ADSP attribute.

AUDITOR | NOAUDITOR

AUDITOR
specifies that the user is to have full responsibility for auditing the use of system resources. An AUDITOR user can control the logging of detected accesses to any RACF-protected resources during RACF authorization checking and accesses to the RACF data set.

You must have the SPECIAL attribute to enter the AUDITOR operand.

NOAUDITOR
specifies that the user no longer has the AUDITOR attribute.

You must have the SPECIAL attribute to enter the NOAUDITOR operand.

AUTHORITY(*group-authority*)
specifies the new level of authority the user is to have in the group specified in the GROUP operand. The valid group authority values are USE, CREATE, CONNECT, and JOIN as described in "Group Authorities" on page 11. If you specify AUTHORITY without *group-authority*, RACF ignores the operand and the existing group authority remains unchanged.

CICS | NOCICS

Note: *This operand applies to z/OS systems only and requires CICS/ESA 3.2.1 or later.*

adds, alters, or deletes CICS operator information for a CICS terminal user.

If you are adding a CICS segment to a user profile, omitting a suboperand is equivalent to omitting the suboperand on the ADDUSER command. If you are changing an existing CICS segment in a user profile, omitting a suboperand leaves the existing value for that suboperand unchanged.

You can control access to the entire CICS segment or to individual fields within the CICS segment by using field level access checking. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

OPCLASS(*operator-class1*,*operator-class2*,...) | NOOPCLASS

where *operator-class1, operator-class2* are numbers in the range of 1 through 24. These numbers represent classes assigned to this operator to which BMS (basic mapping support) messages will be routed.

NOOPCLASS deletes any operator classes from this profile and returns the user to the CICS defaults for this field. This field will no longer appear in LISTUSER output.

OPIDENT(*operator-id*) | NOOPIDENT

specifies a 1-to-3-character identification of the operator for use by BMS.

Operator identifiers may consist of any characters, and may be entered with or without single quotation marks. The following rules hold:

- If parentheses, commas, blanks, or semicolons are to be entered as part of the operator identifier, the character string must be enclosed in single quotation marks. For example, if the operator identifier is `(1)`, you must enter `OPIDENT('(1)')`.
- If a single quotation mark is intended to be part of the operator identifier, and the entire character string is enclosed in single quotation marks, two single quotation marks must be entered together for each single quotation mark within the string. For example, if the operator identifier is `1',` (a one, followed by a single quotation mark, followed by a comma), then you would enter `OPIDENT('1'',')`. Note that the whole string must be within single quotation marks due to the presence of the comma.
- If the first character of the operator identifier is a single quotation mark, then the string must be entered within single quotation marks and two single quotation marks entered for the first character. For example, if the operator identifier is `'12` (a quote followed by a one, followed by a two), you would enter `OPIDENT(''12')`.

NOOPIDENT deletes the operator identification and returns the user to the CICS default for this field.

This field will default to blanks in the RACF user profile, and blanks will appear for the field in LISTUSER output.

OPPRTY(*operator-priority*) | NOOPPRTY

specifies a number in the range of 0 through 255 that represents the priority of the operator.

NOOPPRTY deletes the operator priority and returns the user to the CICS default for this field.

This field will default to zeros in the RACF user profile, and zeros will appear for the field in LISTUSER output.

TIMEOUT(*timeout-value*) | NOTIMEOUT

specifies a number in the range of 0 through 60 that is the time in minutes that the operator is allowed to be idle before being signed off.

If this suboperand is omitted, there is no change to this field.

NOTIMEOUT deletes the timeout value and returns the user to the CICS default for this field.

This field will default to zeros in the RACF user profile, and zeros will appear for the field in LISTUSER output.

XRFSOFF(FORCE | NOFORCE) | NOXRFSOFF
specifies that the user is to be signed off by CICS when an XRF takeover occurs.

N0XRFS0FF returns the user to the CICS default for this field.

This field will default to NOFORCE in the RACF user profile, and NOFORCE will appear in LISTUSER output.

NOCICS
deletes the CICS segment from a user profile. No CICS information will appear in LISTUSER output.

CLAUTH | NOCLAUTH

CLAUTH(*class-name* ...)
specifies the classes in which the user is allowed to define profiles to RACF for protection, in addition to the classes previously allowed for the user. Classes you can specify are USER, and any resource class defined in the class descriptor table. RACF adds any class names you specify to the class names previously specified for this user.

To enter the CLAUTH operand, you must have the SPECIAL attribute, or the user's profile must be within the scope of a group in which you have the group-SPECIAL attribute and have the CLAUTH attribute, or you must be the owner of the user's profile and have the CLAUTH attribute for the class to be added. If you do not have sufficient authority for a specified class, RACF ignores the CLAUTH specification for that class and continues processing with the next class name specified.

Note: The CLAUTH attribute has no meaning for the FILE and DIRECTRY classes.

NOCLAUTH(*class-name* ...)
specifies that the user is not allowed to define profiles to RACF for any *class-names* that you specify. The valid *class-names* are USER and any resource class name defined in the class descriptor table. RACF deletes any class names you specify from the class names previously allowed for this user.

To enter the NOCLAUTH operand, you must have the SPECIAL attribute, or the user's profile must be within the scope of a group in which you have the group-SPECIAL attribute and have the CLAUTH attribute, or you must be the owner of the user's profile and have the CLAUTH attribute for the class to be deleted. If you do not have sufficient authority for a specified class, RACF ignores the NOCLAUTH specification for that class and continues processing with the next class name specified.

DATA | NODATA

DATA('*installation-defined-data*')
specifies up to 255 characters of installation-defined data to be stored in the user's profile. It may contain double-byte character set (DBCS) data and must be enclosed in single quotation marks. Note that only 254 characters will be chained off the ACEE.

Use the LISTUSER command to list this information.

The data is available (in a user's ACEE) to the RACDEF preprocessing installation exit routine, the RACHECK preprocessing and postprocessing installation exit routines, and the RACINIT postprocessing installation exit routines.

NODATA
specifies that the ALTUSER command is to delete the installation-defined data in the user's profile.

DFLTGRP(*group-name*)
specifies the name of a RACF-defined group to be used as the new default group for the user. The user must already be connected to this new group with at least USE authority. The user remains connected to the previous default group.

DFP | NODFP
Note: *These operands apply to z/OS systems only.*

DFP

specifies that, when you change the profile of a user, you can enter any of the following suboperands to add, change, or delete default values for the DFP data application, data class, management class, and storage class. DFP uses this information to determine data management and DASD storage characteristics when a user creates a new data set.

You can control access to the entire DFP segment or to individual fields within the DFP segment by using field level access checking. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

DATAAPPL | NODATAAPPL

DATAAPPL(*application-name*)
specifies the name of a DFP data application. The name you specify can contain up to 8 alphanumeric characters.

NODATAAPPL
specifies that you want to delete the DFP data application name from the DFP segment of the user's profile.

DATACLAS | NODATACLAS

DATACLAS(*data-class-name*)
specifies the default data class. The class name you specify can contain up to 8 alphanumeric characters.

A data class can specify some or all of the physical data set attributes associated with a new data set. During new data set allocation, data management uses the value you specify as a default unless it is preempted by a higher priority default, or overridden in some other way (for example, by JCL).

The value you specify must be a valid data class name defined for use on your system. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

For information on defining DFP data classes, see *MVS/Extended Architecture Storage Administration Reference*.

NODATACLAS
specifies that you want to delete the default data class name from the DFP segment of the user's profile.

MGMTCLAS | NOMGMTCLAS

MGMTCLAS(*management-class-name*)
specifies the default management class. The class name you specify can contain up to 8 alphanumeric characters.

A management class contains a collection of management policies that apply to data sets. Data management uses the value you specify as a default unless it is preempted by a higher priority default, or overridden in some other way (for example, by JCL).

The value you specify must be defined as a profile in the MGMTCLAS general resource class, and the user must be granted at least READ access to the profile. Otherwise, RACF will not allow the user access to the specified MGMTCLAS. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

For information on defining DFP management classes, see *MVS/Extended Architecture Storage Administration Reference*.

NOMGMTCLAS
specifies that you want to delete the default management class name from the DFP segment of the user's profile.

STORCLAS | NOSTORCLAS

STORCLAS(*storage-class-name*)
specifies the default storage class. The class name you specify can contain up to 8 alphanumeric characters.

A storage class specifies the service level (performance and availability) for data sets managed by the storage management subsystem (SMS). During new data set allocation, data management uses the value you specify as a default unless it is preempted by a higher priority default, or overridden in some other way (for example, by JCL).

The value you specify must be defined as a profile in the STORCLAS general resource class, and the user must be granted at least READ access to the profile. Otherwise, RACF will not allow the user access to the specified STORCLAS. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

For information on defining DFP storage classes, see *MVS/Extended Architecture Storage Administration Reference*.

NOSTORCLAS
specifies that you want to delete the default storage class name from the DFP segment of the user's profile.

NODFP
specifies that RACF should delete the DFP segment from the user's profile.

EXPIRED | NOEXPIRED

EXPIRED
Specifies that the new password or password phrase specified be marked as expired. This requires the user to change it at the next logon.

When EXPIRED is specified without the PASSWORD or PHRASE keyword, the existing password and password phrase (if they exist) are marked as expired.

When EXPIRED is specified with the PHRASE keyword, the phrase you specify is subject to the basic RACF rules for password phrase syntax and to any rules set by the installation through the new-password-phrase exit (ICHPWX11), if present.

When EXPIRED is specified with the PASSWORD keyword, the password you specify is *not* subject to the password syntax rules set by the installation through the SETROPTS PASSWORD command. However, the password is checked by the new-password exit (ICHPWX01), if present.

NOEXPIRED
Specifies that the password specified by the PASSWORD keyword or the password phrase specified by the PHRASE keyword need not be changed at the next logon. The NOEXPIRED keyword is only valid when specified with the PASSWORD or PHRASE keyword. NOEXPIRED does *not* indicate that the password or password phrase never expires. If you wish to set a password or password phrase that never expires, use the NOINTERVAL keyword on the PASSWORD command.

When NOEXPIRED is specified, the value supplied is subject to certain rules. Those rules include the basic RACF rules for password phrase syntax and any rules set by the installation through the SETROPTS PASSWORD command.

The new password exit (ICHPWX01), if present is called to check passwords. The new-password-phrase exit (ICHPWX11), if present, is called to check password phrases and perform additional validation.

To specify NOEXPIRED, you must have the SPECIAL attribute (at the system level) or you must have UPDATE access to either the IRR.PASSWORD.RESET resource or the appropriate IRR.PWRESET resource in the FACILITY class. Being the owner of the USER profile or having the group-SPECIAL attribute is *not* sufficient when NOEXPIRED is specified.

GROUP(*group-name*)
specifies the name of a group that the user is connected to.

Changes to the group-related user attributes UACC and AUTHORITY are applied to the specified group. The user must be connected to the specified group, for changes to apply to that userid.

If you omit GROUP, the changes apply to the user's default group. If you omit GROUP and specify DFLTGRP, however, the changes still apply to the user's previous default group. To have the changes apply to the newly specified default group, you must log off and log on once again.

GRPACC | NOGRPACC

Note: *These operands apply to z/OS systems only.*

GRPACC
specifies that any group data sets protected by DATASET profiles defined by this user will be automatically accessible to other users in the group. The group whose name is used as the high-level qualifier of the data set name (or the qualifier supplied by a command installation exit) will have UPDATE access authority in the new profile. GRPACC specified on the ALTUSER command overrides NOGRPACC specified on the CONNECT command.

NOGRPACC
specifies that the user no longer has the GRPACC attribute.

LANGUAGE| NOLANGUAGE

Note: *These operands apply to z/OS systems only.*

adds, alters, or deletes a user's preferred national languages.

Specify LANGUAGE if this user is to have languages other than the installation defaults (established by the LANGUAGE operand on the SETROPTS command). Specify NOLANGUAGE to delete a user's preferred national languages and to return that user to the installation defaults.

LANGUAGE(PRIMARY(*language*) SECONDARY(language))
specifies, for the PRIMARY and SECONDARY languages, either the installation-defined name of a currently active language (a maximum of 24 characters) or one of the language codes (3 characters in length) for a language installed on your system.

- If this profile is for a TSO/E user who will establish an extended MCS console session, the languages you specify should be one of the languages specified on the LANGUAGE LANGCODE statements in the MMSLSTxx PARMLIB member. See your z/OS system programmer for this information.

  For more information on TSO/E national language support, see *TSO/E Customization*.
- If this profile is for a CICS user, see your CICS administrator for the languages supported by CICS on your system.

  For more information, see *CICS-RACF Security Guide*.

PRIMARY(*language*) | NOPRIMARY
specifies the user's new primary language.

The language name may be a quoted or unquoted string. The *language* variable must be either the installation-defined name of a currently active language (a maximum of 24 characters) or one of the language codes (3 characters in length) for a language installed on your system.

NOPRIMARY deletes any primary language information from the user's profile and returns the user to the installation's default primary language.

SECONDARY(*language*) | NOSECONDARY
specifies the language to which the user's secondary language is to be changed.

The language name may be a quoted or unquoted string. The *language* variable must be either the installation-defined name of a currently active language (a maximum of 24 characters) or one of the language codes (3 characters in length) for a language installed on your system.

NOSECONDARY deletes any secondary language information from the user's profile and returns the user to the installation's default secondary language.

Note:

1. The same language can be specified for both PRIMARY and SECONDARY.
2. If RACF is not running under MVS/ESA SP 4.1 or later, or if the z/OS message service is not active, or if RACF is running under z/VM, the PRIMARY and SECONDARY values must be a 3-character language code.

NOLANGUAGE
deletes the user's preferred national languages from the profile. LANGUAGE information will no longer appear in LISTUSER output.

MFA([PWFALLBACK | NOPWFALLBACK]) | NOMFA
enables or disables Multi-Factor Authentication (MFA) for the user. Note that a protected user is created only when the user has no password, no passphrase, and is not enabled for MFA.

PWFALLBACK
specifies the user is allowed to use the FALLBACK command parameter on the z/VM LOGON command. FALLBACK enables the traditional RACF authentication methods (password, passphrase, etc.) to be in effect for a valid LOGON FALLBACK request.

NOPWFALLBACK
specifies the user is not allowed to use the FALLBACK command parameter on the z/VM LOGON command. That is, LOGON via MFA will always be required, and the request will be denied should MFA fail or be unavailable. NOPWFALLBACK is the default.

NOMFA
disables MFA for the user.

MODEL | NOMODEL
Note: *These operands apply to z/OS systems only.*

MODEL(*dsname*)
specifies the name of a data set that RACF is to use as a model when new data set profiles are created that have *userid* as the high-level qualifier. For this operand to be effective, the MODEL(USER) option (specified on the SETROPTS command) must be active. If the ALTUSER command cannot find the *dsname* profile, it issues a warning message but places the model name in the userid entry.

Note that RACF always prefixes *dsname* with the user ID.

For information about automatic profile modeling, refer to *z/VM: RACF Security Server Security Administrator's Guide*.

NOMODEL
deletes the model profile name in the user's profile.

NAME('*user-name*')
specifies the new user name to be associated with the user ID. You can use a maximum of any 20 characters. If the name you specify contains any blanks, it must be enclosed in single quotation marks.

OPERATIONS | NOOPERATIONS

OPERATIONS
on z/OS, specifies that the user is to have authorization to do maintenance operations on all RACF-protected DASD data sets, tape volumes, and DASD volumes except those where the access list specifically limits the OPERATIONS user to an access authority that is less than the operation requires.

On z/VM, the OPERATIONS attribute allows the user to access z/VM resources except those where the access list specifically limits the OPERATIONS user to a lower access authority.

You establish the lower access authority for the OPERATIONS user with the PERMIT command. OPERATIONS on the ALTUSER command overrides NOOPERATIONS on the CONNECT command.

You must have the SPECIAL attribute to use the OPERATIONS operand.

NOOPERATIONS
specifies that the user no longer has the OPERATIONS attribute.

You must have the SPECIAL attribute to use the NOOPERATIONS operand.

OPERPARM | NOOPERPARM

Note: *These operands apply to z/OS systems only.*

specifies or deletes default information used when this user establishes an extended MCS console session.

You can control access to the entire OPERPARM segment or to individual fields within the OPERPARM segment by using field level access checking. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

For information on planning how to use OPERPARM segments, see *MVS/ESA Planning: Operations*.

Note:

1. You need not specify every suboperand in an OPERPARM segment. In general, if you omit a suboperand, the default is the same as the default in the CONSOLxx PARMLIB member, which can also be used to define consoles.
2. If you specify MSCOPE or ROUTCODE but do not specify a value for them, RACF uses MSCOPE(*ALL) and ROUTCODE(NONE) to update the corresponding fields in the user profile. These values will appear in listings of the OPERPARM segment of the user profile.
3. If you omit the other suboperands, RACF will not update the corresponding fields in the user's profile, and no value will appear in listings of the OPERPARM segment of the profile.

ALTGRP(*alternate-console-group*) | NOALTGRP

specifies the console group used in recovery.

The variable *alternate-console-group* can be 1 to 8 characters in length, with valid characters being 0 through 9, A through Z, # (X'7B'), $ (X'5B'), or @ (X'7C').

NOALTGRP deletes alternate console group information from this profile.

AUTH(MASTER | ALL | INFO | any others) | NOAUTH

specifies or deletes this console's authority to issue operator commands.

If you omit this operand, RACF will not alter this field in the user's profile. If this field has not been added to the user's profile, an extended MCS console will use AUTH(INFO) when a session is established.

The console can have the following authorities:

MASTER

allows this console to act as a master console, which can issue all z/OS operator commands. This authority can only be specified by itself.

ALL

allows this console to issue system control commands, input/output commands, console control commands, and informational commands. This authority can only be specified by itself.

INFO

allows this console to issue informational commands. This authority can only be specified by itself.

CONS

allows this console to issue console control and informational commands.

IO

allows this console to issue input/output and informational commands.

SYS

allows this console to issue system control commands and informational commands.

NOAUTH
deletes the user's operator authorities from the profile. Console operator authority will no longer appear in profile listings. However, AUTH(INFO) will be used when an extended MCS console session is established.

AUTO(YES | NO) | NOAUTO
specifies whether the extended console can receive messages which have been automated by the Message Processing Facility (MPF) in the sysplex.

NOAUTO deletes this field from the user's profile. AUTO information will no longer appear in profile listings. However, AUTO(NO) will be used when an extended MCS console session is established.

CMDSYS(*system-name* | *) | NOCMDSYS
specifies the system to which commands from this console are to be sent.

If you omit this operand, RACF does not alter this field in the user's profile. If this field has not been added to the user's profile, an extended MCS console will use CMDSYS(*) when a session is established. The variable *system-name* must be 1 to 8 characters (A through Z, 0 through 9, and @ (X'7C'), # (X'7B'), $ (X'5B'). If * is specified, commands are processed on the local system where the console is attached.

NOCMDSYS deletes any system-names from this profile. No CMDSYS information will appear in profile listings. However, CMDSYS(*) will be used when an extended MCS console session is established.

DOM(NORMAL | ALL | NONE) | NODOM
specifies which delete operator message (DOM) requests this console can receive.

If you omit this operand, RACF does not alter this field in the user's profile. If this field has not been added to the user's profile, an extended MCS console will use DOM(NORMAL) when a session is established.

NORMAL
The system queues all appropriate DOM requests to this console.

ALL
All systems in the sysplex queue DOM requests to this console.

NONE
No DOM requests are queued to this console.

NODOM deletes this field from the user's profile. DOM information will no longer appear in profile listings. However, DOM(NORMAL) will be used when an extended MCS console session is established.

KEY(*searching-key*) | NOKEY
specifies a 1 to 8 byte character name that can be used to display information for all consoles with the specified key by using the z/OS command, DISPLAY CONSOLES,KEY. If specified, KEY can include A through Z, 0 through 9, #(X'7B'), $(X'5B'), or @(X'7C').

If you omit this operand, RACF does not alter this field in the user's profile. If this field has not been added to the user's profile, an extended MCS console will use a KEY value of NONE when a session is established.

NOKEY deletes search key information from the user's profile. Search key information will no longer appear in profile listings. However, a KEY value of NONE is used when an extended MCS console session is established.

LEVEL(*message-level*) | NOLEVEL
specifies the messages that this console is to receive.

If you omit this operand, RACF does not alter this field in the user's profile. If this field has not been added to the user's profile, an extended MCS console will use LEVEL(ALL) when a session is established.

The *message-level* variable can be a list of R, I, CE, E, IN, NB or ALL. If you specify ALL, you cannot specify R, I, CE, E, or IN.

NB
The console receives *no* broadcast messages.

ALL
The console receives these messages: R, I, CE, E, IN.

R
The console receives messages requiring an operator reply.

I
The console receives immediate action messages.

CE
The console receives critical eventual action messages.

E
The console receives eventual action messages.

IN
The console receives informational messages.

NOLEVEL deletes any defined message levels for this console from the profile. Message information will no longer appear in profile listings. However, LEVEL(ALL) will be used when an extended MCS console session is established.

LOGCMDRESP(SYSTEM | NO) | NOLOGCMDRESP
specifies if command responses are to be logged.

If you omit this operand, RACF does not alter this field in the user's profile. If this field has not been added to the user's profile, an extended MCS console will use LOGCMDRESP(SYSTEM) when a session is established.

SYSTEM
command responses are logged in the hardcopy log.

NO
command responses are not logged.

NOLOGCMDRESP deletes the value for LOGCMDRESP from the profile. Command response logging information will no longer appear in profile listings. However, “LOGCMDRESP(SYSTEM)” will be used when an extended MCS console session is established.

MFORM(*message-format*) | NOMFORM
specifies the format in which messages are displayed at the console.

If you omit this operand, RACF does not alter this field in the user's profile. If this field has not been added to the user's profile, an extended MCS console will use MFORM(M) when a session is established.

The *message-format* variable can be a combination of T, S, J, M, and X.

J
Messages are displayed with a job ID or name.

M
The message text is displayed.

S
Messages are displayed with the name of the originating system.

T
Messages are displayed with a time stamp.

X
Messages that are flagged as exempt from job name and system name formatting are ignored.

NOMFORM deletes the values for MFORM from the profile and causes message text to be displayed (MFORM(M)) when an extended MCS console session is established.

MIGID(YES | NO) | NOMIGID
specifies whether a 1-byte migration ID is to be assigned to this console or not. The migration ID allows command processors that use a 1-byte console ID to direct command responses to this console.

If you omit this operand, RACF does not alter this field in the user's profile. If this field has not been added to the user's profile, an extended MCS console will use MIGID(NO) when a session is established.

NOMIGID deletes this segment from the profile. Migration identification information will no longer appear in profile listings. However, MIGID(NO) will be assigned when an extended MCS console session is established.

MONITOR(*events*) | NOMONITOR
specifies which information should be displayed when monitoring jobs, TSO sessions, or data set status.

If you omit this operand, RACF does not alter this field in the user's profile. If this field has not been added to the user's profile, an extended MCS console will use MONITOR(JOBNAMES SESS) when a session is established. The variable *events* can be a list of the following:

JOBNAMES | JOBNAMEST
displays information about the start and end of each job. JOBNAMES omits the times of job start and job end. JOBNAMEST displays the times of job start and job end.

SESS | SESST
displays information about the start and end of each TSO session. SESS omits the times of session start and session end. SESST displays the times of session start and session end.

STATUS
specifies that the information displayed when a data set is freed or unallocated should include the data set status.

NOMONITOR deletes job monitor information from the user's profile. Information from this field will no longer appear in profile listings. However, MONITOR(JOBNAMES SESS) will be used when an extended MCS console session is established.

MSCOPE(*system-names* | * | *ALL) | NOMSCOPE
specifies the systems from which this console can receive messages that are not directed to a specific console.

If you omit this operand, RACF does not alter this field in the user's profile. If this field has not been added to the user's profile, an extended MCS console will use MSCOPE(*ALL) when a session is established. If you specify MSCOPE but omit a value, RACF uses MSCOPE(*ALL) to update this field in the user's profile. *ALL will appear in listings of the OPERPARM segment of the user's profile.

system-names
is a list of one or more system names, where a system name can be any combination of A through Z, 0 through 9, # (X'7B'), $ (X'5B'), or @ (X'7C').

***
is the system on which the console is currently active.

***ALL**
means all systems.

NOMSCOPE deletes any system name information from the user's profile. Message reception information will no longer appear in profile listings. However, MSCOPE(*ALL) will be used when an extended MCS console session is established.

ROUTCODE(ALL | NONE | *routing-codes*) | NOROUTCODE
specifies the routing codes of messages this operator is to receive.

If you omit this operand, RACF does not alter this field in the user's profile. If this field has not been added to the user's profile, an extended MCS console will use ROUTCODE(NONE) when a session is established. If you specify ROUTCODE but omit a value, RACF uses ROUTCODE(NONE) to update this field in the user's profile. NONE will appear in listings of the OPERPARM segment of the user's profile.

The routing code information can be one of the following:

ALL
means all routing codes.

NONE
means no routing codes.

routing-codes
specifies one or more routing codes or sequences of routing codes. The routing codes can be list of n and n1:n2, where n, n1, and n2 are integers from 1 to 128, and n2 is greater than n1.

NOROUTCODE deletes routing code information from the user's profile. Routing code information will no longer appear in profile listings. However, ROUTCODE(NONE) will be used when an extended MCS console session is established.

STORAGE(*amount*) | NOSTORAGE
specifies the amount of storage in the TSO/E user's address space that can be used for message queuing to this console.

If you omit this operand, RACF does not alter this field in the user's profile. If this field has not been added to the user's profile, an extended MCS console will use STORAGE(1) when a session is established. A value of 0 will appear in listings of the user's profile to indicate that no value was specified. The variable *amount* must be a value between 1 and 2000.

NOSTORAGE deletes this field from the profile. A value of 0 will appear in listings of the user's profile to indicate that no value was specified. However, STORAGE(1) will be used when an extended MCS console session is established.

UD(YES | NO) | NOUD
specifies whether this console is to receive undelivered messages.

If you do not specify this operand, RACF does not alter the user's profile. If this field has not been added to the user's profile, an extended MCS console will use UD(NO) when a session is established.

NOUD deletes the field from the profile. Undelivered message information will no longer appear in profile listings. However, UD(NO) will be used when an extended MCS console session is established.

NOOPERPARM
specifies that the OPERPARM segment is to be deleted. Operator information will no longer appear in LISTUSER output.

OVM | NOOVM

OVM
specifies OpenExtensions information for the user profile being changed.

You can control access to the entire OVM segment or to individual fields within the OVM segment by using field-level access checking.

FSROOT | NOFSROOT

FSROOT(*file-system-root*)
specifies the pathname for the file system root.

When you define the FSROOT pathname to RACF, it can be from 1 to 1023 characters. The FSROOT pathname can consist of any characters and can be entered with or without single quotation marks. The following rules apply:

- If parentheses, commas, blanks, or semicolons are to be entered as part of the pathname, the character string must be enclosed in single quotation marks.
- If a single quotation mark is intended to be part of the pathname and the entire character string is enclosed in single quotation marks, two single quotation marks must be entered together for each single quotation mark within the string.
- If the first character of the pathname is a single quotation mark, then the string must be entered within single quotation marks and two single quotation marks entered for the first character.

Both uppercase and lowercase are accepted and maintained in the case in which they are entered. The fully-qualified pathname should be specified. RACF does not ensure that a valid pathname has been specified.

The z/VM command line will not allow you to enter a pathname as long as 1023 characters. See “RAC (Enter RACF Commands on z/VM)” on page 207 for instructions on entering a long RACF command.

NOFSROOT
specifies that you want to delete the FSROOT pathname from the OVM segment of the user's profile.

If no value is specified for FSROOT in the OVM segment, z/VM sets the file system root for the user to the value specified in the CP directory. If no value is specified in the CP directory, the user has to issue the OPENVM MOUNT command to mount the appropriate file system.

HOME | NOHOME

HOME(*initial-directory-name*)
specifies the file system initial directory pathname. The initial directory is part of the file system. This will be the current working directory.

When you define a HOME pathname to RACF, it can be from 1 to 1023 characters. The HOME pathname can consist of any characters and can be entered with or without single quotation marks. The following rules apply:

- If parentheses, commas, blanks, or semicolons are to be entered as part of the pathname, the character string must be enclosed in single quotation marks.
- If a single quotation mark is intended to be part of the pathname, and the entire character string is enclosed in single quotation marks, two single quotation marks must be entered together for each single quotation mark within the string.
- If the first character of the pathname is a single quotation mark, then the string must be entered within single quotation marks and two single quotation marks entered for the first character.

Both uppercase and lowercase are accepted and maintained in the case in which they are entered. The fully-qualified pathname should be specified. RACF does not ensure that a valid pathname has been specified.

The z/VM command line will not allow you to enter a pathname as long as 1023 characters. See “RAC (Enter RACF Commands on z/VM)” on page 207 for instructions on entering a long RACF command.

NOHOME
specifies that you want to delete the initial directory pathname from the OVM segment of the user's profile.

If no value is specified for HOME in the OVM segment, z/VM will use the value specified in the CP directory. If no value is specified in the CP directory, z/VM will set the working directory for the user to “/” (the root directory).

PROGRAM | NOPROGRAM

PROGRAM(*program-name*)
specifies the PROGRAM pathname (shell program). This will be the first program started when the OPENVM SHELL command is entered.

When you define a PROGRAM pathname to RACF, it can be from 1 to 1023 characters. The PROGRAM pathname can consist of any characters and can be entered with or without single quotation marks. The following rules apply:

- If parentheses, commas, blanks, or semicolons are to be entered as part of the pathname, the character string must be enclosed in single quotation marks.
- If a single quotation mark is intended to be part of the pathname, and the entire character string is enclosed in single quotation marks, two single quotation marks must be entered together for each single quotation mark within the string.
- If the first character of the pathname is a single quotation mark, then the string must be entered within single quotation marks and two single quotation marks entered for the first character.

Both uppercase and lowercase are accepted and maintained in the case in which they are entered. The fully-qualified pathname should be specified. RACF does not ensure that a valid pathname has been specified.

The z/VM command line will not allow you to enter a pathname as long as 1023 characters. See "RAC (Enter RACF Commands on z/VM)" on page 207 for instructions on entering a long RACF command.

NOPROGRAM
specifies that you want to delete the OpenExtensions program pathname from the OVM segment of the user's profile.

If no value is specified for PROGRAM in the OVM segment, z/VM uses the value specified in the CP directory. If no value is specified in the CP directory, z/VM gives control to the default shell program (/bin/sh) when a user issues the OPENVM SHELL command.

UID | NOUID

UID(*user-identifier*)
specifies the user identifier. The UID is a numeric value between 0 and 2 147 483 647.

Be careful about assigning 0 as the user identifier. A UID of 0 is considered a superuser. The superuser will pass all OpenExtensions security checks.

Note:

1. RACF does not require the UID to be unique. The same value can be assigned to multiple users, but this is not recommended because individual user control would be lost. However, if you want a set of users to have exactly the same access to the OpenExtensions resources, you may decide to assign the same UID to more than one user.
2. Be careful when changing the UID for a user. The following situations may occur.
   - If the file system contains files created by a user and contains the user's old UID as the file owner UID, the user will lose access to those files, depending on the permission bits associated with the file.
   - If files already exist with an owner UID equal to the user's new UID value, the user will gain access to these files.
   - If another user is subsequently given the old value as its UID, this user will have access to the old files.
   - If you have an EXEC.U*uid* profile in the VMPOSIX class for the old UID value, make sure you delete this profile and create another to reflect the new value. For an explanation of these profiles, see *z/VM: RACF Security Server Security Administrator's Guide*.

NOUID
specifies that you want to delete the user identifier from the OVM segment of the user's profile.

If NOUID is specified, the user will be assigned the default UID of 4 294 967 295 (X'FFFFFFFF'). The LISTUSER command displays the field name followed by the word “NONE”.

NOOVM
specifies that RACF should delete the OVM segment from the user's profile.

OWNER(*userid* or *group-name*)
specifies a RACF-defined user or group to be assigned as the new owner of the user's profile.

PASSWORD | NOPASSWORD

PASSWORD(*password*)
specifies the user's logon password. Use this command to specify a password for a user who has forgotten his/her password. Unless the NOEXPIRED operand is also specified, this password is set expired, thus requiring the user to change the password at next logon. Note that the password syntax rules your installation defines using SETROPTS PASSWORD do not apply to this password unless the NOEXPIRED operand is also included. (See the NOEXPIRED operand.)

Note:

1. If the installation is maintaining user password history, the password that was in effect prior to issuing this command is stored as part of this history. Note that the password specified is not subject to history checking.
2. When the installation specifies a minimum change interval, RACF checks the number of days between password changes to ensure the minimum required days have elapsed each time users change their own passwords. RACF also checks the days when users change passwords using their IRR.PASSWORD.RESET or IRR.PWRESET authority unless the command issuer has CONTROL authority or higher.

NOPASSWORD
specifies that the user does not have a password which can be used to authenticate the user. This allows you the option of defining a user which can only authenticate by using a password phrase and/or MFA, which are generally both stronger than a password.

Specifying a user as a NOPASSWORD user can also be used as an extra safeguard for service machine user IDs which are not meant to be logged on to directly. When a user has no password, no password phrase, and is not enabled for MFA, the user is a protected user. If a protected user attempts to enter the system with a password, a password phrase, or MFA, the attempt fails. However, the user ID is not revoked due to the failed password attempts even if the SETROPTS PASSWORD(REVOKE) option is in effect.

The ability to define a "phrase-only" user and/or "MFA-only" user depends on whether the user uses any applications which check passwords, and which do not support password phrases or MFA. See the descriptions of the MFA operand above and the PHRASE operand below.

Note:

1. Protected user IDs can only enter the system by means of an AUTOLOG or XAUTOLOG command, and are protected from being revoked through inactivity or unsuccessful attempts to access the system using incorrect passwords, password phrases, and MFA credentials. The PROTECTED attribute will appear in LISTUSER output for any such user. See *z/VM: RACF Security Server Security Administrator's Guide* for more information.
2. The NOPASSWORD attribute will appear in LISTUSER output for any user without a password but with a password phrase.
3. The PASSDATE field will be displayed as "N/A" for any user without a password.

4. Specifying NOPASSWORD will suppress the ICH01022I message which is issued by ADDUSER if neither PASSWORD nor NOPASSWORD is specified.

PHRASE | NOPHRASE

PHRASE(*'password phrase'*)
Specifies the user's password phrase. The password phrase you define is a text string of up to 100 characters and must be enclosed in single quotation marks. By default, the password phrase must be at least 14 characters long, but can be as short as 9 characters if the new-password-phrase exit (ICHPWX11) allows it. Unless the NOEXPIRED operand is also specified, the password phrase is set expired, requiring the user to change it on next use.

The following syntax rules apply to all password phrases. You cannot alter these syntax rules. You cannot add additional rules of your own unless your installation tailors the new-password-phrase exit (ICHPWX11). For programming details, see *z/VM: RACF Security Server System Programmer's Guide*

Password Phrase Syntax Rules

- Must not contain the user ID (as sequential uppercase or sequential lowercase characters)
- Must contain at least 2 alphabetic characters (A-Z, a-z)
- Must contain at least 2 non-alphabetic characters (numerics, punctuation, or special characters)
- Must not contain more than 2 consecutive characters that are identical
- Must be enclosed in single quotation marks, with single quotation marks within the password phrase doubled
- Must not contain forward slashes, nulls (X'00'), or leading or trailing blanks

If ICHPWX11 is present, it can reject the specified password phrase. Password phrases shorter than 14 characters will be rejected by RACF unless ICHPWX11 is present and allows the new value.

If the specified password phrase is accepted, it is made the user's current password phrase and, when SETROPTS PASSWORD(HISTORY) is in effect, it is added to the user's password phrase history. Note that the specified password phrase is not subject to history checking.

If you omit PHRASE, no password phrase is assigned. If you enter PHRASE without a password phrase value, you are prompted for a value if you are in a RACF command session.

The PASSPHRASE attribute will appear in LISTUSER output for any user who has been assigned a password phrase.

When the installation specifies a minimum change interval, RACF checks the number of days between password phrase changes to ensure the minimum required days have elapsed each time users change their own password phrases. RACF also checks the days when users change password phrases using the IRR.PASSWORD.RESET or IRR.PWRESET authority unless the command issuer has CONTROL authority or higher.

NOPHRASE
Specifies that the user cannot use a password phrase for authentication. If a password phrase was previously set, the password phrase is cleared. The date of the password phrase change is also cleared from the user's profile. See “NOPASSWORD ” on page 113 for more information on NOPASSWORD/NOPHRASE users.

PWCLEAN
performs the following functions:

- Removes residual password and password phrase history entries resulting from lowering the SETROPTS PASSWORD(HISTORY(*n*)) value.
- Reorganizes the history so that an increase in the SETROPTS PASSWORD(HISTORY(*n*)) value takes immediate effect.

- Removes any password history and password phrase history from a PROTECTED user.

You must have the SPECIAL attribute to use the PWCLEAN operand.

When the SETROPTS PASSWORD(HISTORY(*n*)) value is lowered, the residual history entries continue to be used by RACF. PWCLEAN removes these entries.

If the SETROPTS PASSWORD(HISTORY(*n*)) value is raised, the higher number does not immediately take effect, depending on how many times a user has changed their password or password phrase in the past. PWCLEAN reorganizes the history so that the history change takes effect immediately after using PWCLEAN.

PWCLEAN should be used against all user IDs whenever the SETROPTS PASSWORD(HISTORY(*n*)) value is changed. The SEARCH command with the CLIST option provides a way of creating a "utility" to do this.

PWCONVERT
performs the following functions:

- Performs the PWCLEAN function.
- If KDFAES is active:
  - If the current password is in legacy format, converts it to KDFAES format.
  - Converts any legacy-format password history entries to KDFAES.
- If KDFAES is not active:
  - Deletes any password and password phrase history entries that are in KDFAES format.

You must have the SPECIAL attribute to use the PWCONVERT operand.

PWCONVERT does nothing with the current password phrase. After KDFAES is enabled, the phrase must be changed before it is encrypted with the new algorithm. Likewise, PWCONVERT does nothing with phrase history entries. They remain in their legacy form until they are replaced in the history.

The IRRDBU00 utility reports on the algorithm that is used to encrypt a user's current password and password phrase, including the number of legacy password history entries. This information can be used to determine the exact user IDs needing an update. This allows for a more efficient conversion than SEARCH with CLIST.

Attention:

1. The existing current password and password history entries are assumed to be encrypted with DES when PWCONVERT encrypts them using KDFAES. If you use masking, or an installation-defined encryption method by use of an ICHDEX01 exit, do not use PWCONVERT. This results in the user being unable to log on until the password is changed. In addition, it results in unusable history entries. That is, a user is able to reuse a password value that is contained in the password history.
2. When password history entries are converted, they can never be converted back to the legacy format. Thus, they are always more expensive to evaluate, and they are not recognized by any systems not containing KDFAES support.

RESUME | NORESUME

RESUME[(*date*)]
specifies that the user is to be allowed to access the system again. You normally use RESUME to restore access to the system that has been prevented by a prior REVOKE.

If you specify a date, RACF does not allow the user to access the system until the date you specify. The date must be a future date; if it is not, you are prompted to provide a future date.

During the time between when you specify the RESUME and the date when the RESUME takes effect, the RESUME is called a pending RESUME. You specify a date in the form mm/dd/yy, and you need not specify leading zeros; specifying 9/1/92 is the same as specifying 09/01/92.

If you specify RESUME without a date, the RESUME takes effect immediately. Specifying RESUME without a date overrides any pending RESUME and any pending REVOKE.

When no REVOKE or pending REVOKE is in effect for the user, the RESUME operand causes RACF to reset the user's inactivity timer by updating the user's last access date.

Note:

1. If you use the ALTUSER command to issue a REVOKE for a user, you must use the ALTUSER command to issue the corresponding RESUME. Issuing RESUME on the CONNECT command does not restore access revoked on the ALTUSER command.
2. If you specify both REVOKE(*date*) and RESUME(*date*), RACF acts on them in date order. For example, if you specify RESUME(8/19/06) and REVOKE(8/5/06), RACF prevents the user from accessing the system from August 5, 2006, to August 18, 2006. On August 19, the user can again access the system.

   If a user is already revoked and you specify RESUME(8/5/06) and REVOKE(8/19/06), RACF allows the user to access the system from August 5, 2006, to August 18, 2006. On August 19, RACF prevents the user from accessing the system.
3. If RACF detects a conflict between REVOKE and RESUME (for example, you specify both without a date), RACF uses REVOKE. If you specify, without a date, only REVOKE or only RESUME, RACF clears both date fields. When RACF revokes a user because of inactivity or invalid password attempts, RACF also clears both date fields.
4. To clear the RESUME date field, specify NORESUME.
5. To successfully resume a user whose revoke date has passed, you must specify NOREVOKE to clear the revoke date as well as specifying the RESUME keyword.
6. Downlevel systems sharing the RACF database should not be affected by the changes to REVOKE and RESUME processing.

NORESUME
Specifies that RACF is to clear the user's RESUME date field. You can use the NORESUME option to cancel the pending resumption (of a user's ID) that resulted from a previous ALTUSER command specified with RESUME(*date*).

REVOKE | NOREVOKE

REVOKE[(*date*)]
specifies that RACF is to prevent the user from accessing the system; the user's profile and data sets, however, are not deleted from the RACF data set.

If you specify a date, RACF does not prevent the user from accessing the system until the date you specify. The date must be a future date; if it is not, you are prompted to provide a future date.

You specify a date in the form mm/dd/yy, where mm is the month, dd is the day, and yy is the year. You need not specify leading zeros; 9/1/92 is the same as 09/01/92. During any time between when you specify the REVOKE and the date when the REVOKE takes effect, the REVOKE is called a pending revoke.

Note: RACF interprets date fields as:

20*yy* when the year is less than 71
19*yy* when the year is 71 or higher

When you specify REVOKE without a date, the following conditions apply:

- The REVOKE takes effect the next time the user tries to log onto the system.
- Any pending RESUME date remains in effect unless you also specify NORESUME.

  Note: To permanently revoke system access, specify both REVOKE and NORESUME.

When a REVOKE is already in effect for the user, RACF ignores the REVOKE operand and issues a message.

Note:

1. Specifying REVOKE on the ALTUSER command overrides RESUME on the CONNECT command.
2. If you specify both REVOKE(*date*) and RESUME(*date*), RACF acts on them in date order. For example, if you specify RESUME(8/19/92) and REVOKE(8/5/92), RACF prevents the user from accessing the system from August 5, 1992, to August 18, 1992. On August 19, the user can again access the system.

   If a user is already revoked and you specify RESUME(8/5/92) and REVOKE(8/19/92), RACF allows the user to access the system from August 5, 1992, to August 18, 1992. On August 19, RACF prevents the user from accessing the system.
3. If RACF detects a conflict between REVOKE and RESUME (for example, you specify both without a date), RACF uses REVOKE. If you specify, without a date, only REVOKE or only RESUME, RACF clears both date fields. When RACF revokes a user because of inactivity or invalid password attempts, RACF also clears both date fields.
4. To clear the REVOKE date field, specify NOREVOKE.
5. Downlevel systems sharing the RACF database should not be affected by the changes to REVOKE and RESUME processing.

NOREVOKE
Specifies that RACF is to clear the user's REVOKE date field. You can use the NOREVOKE option to cancel the pending revocation (of a user's ID) that resulted from a previous ALTUSER command specified with REVOKE(*date*).

To successfully resume a user whose revoke date has passed, you must specify NOREVOKE to clear the revoke date as well as specifying the RESUME keyword.

The NOREVOKE option does not resume the user ID after it was revoked by the ALTUSER REVOKE command or the user's excessive attempts to use incorrect passwords or password phrases.

ROAUDIT | NOROAUDIT

ROAUDIT
Specifies that the user is to have full responsibility for auditing the use of system resources.

You must have the SPECIAL attribute to enter the ROAUDIT operand.

NOROAUDIT
Specifies that the user no longer has the ROAUDIT attribute.

You must have the SPECIAL attribute to enter the NOROAUDIT operand.

SECLABEL | NOSECLABEL

SECLABEL(*seclabel-name*)
specifies the user's default security label where *seclabel-name* is an installation-defined security label that represents an association between a particular security level and a set of zero or more security categories.

A security label corresponds to a particular security level (such as CONFIDENTIAL) with a set of zero or more security categories (such as PAYROLL or PERSONNEL).

For a list of security labels that you can use, enter:

```
SEARCH CLASS(SECLABEL)
```

When the SECLABEL class is not active, RACF ignores this operand. When no member of the SECLABEL profile exists for *seclabel-name*, you are prompted to provide a valid security label name.

NOSECLABEL
specifies that the ALTUSER command is to delete any security label contained in the user profile. The user no longer has access to any resource that requires a requester to have a certain security label.

SECLEVEL | NOSECLEVEL

SECLEVEL(*seclevel-name*)
specifies the user's security level, where *seclevel-name* is an installation-defined name that must be a member of the SECLEVEL profile in the SECDATA class. The security level name that you specify corresponds to the number of the minimum security level that a user must have to access the resource.

When you specify SECLEVEL and the SECDATA class is active, RACF adds security level access checking to its other authorization checking. If global access checking does not grant access, RACF compares the security level allowed in the user profile with the security level required in the resource profile. If the security level in the user profile is less than the security level in the resource profile, RACF denies the access. If the security level in the user profile is equal to or greater than the security level in the resource profile, RACF continues with other authorization checking.

Note: RACF does not perform security level checking for a started procedure with the privileged attribute.

When the SECDATA class is not active, RACF ignores this operand. When the SECLEVEL profile does not include a member for *seclevel-name*, you are prompted to provide a valid security level name.

NOSECLEVEL
specifies that the ALTUSER command is to delete any security level contained in the user profile. The user no longer has access to any resource that requires a requester to have a certain security level.

SPECIAL | NOSPECIAL

SPECIAL
specifies that the user is to be allowed to issue all RACF commands with all operands except the operands that require the AUDITOR attribute. SPECIAL specified on the ALTUSER command overrides NOSPECIAL specified on the CONNECT command.

You must have the SPECIAL attribute to use the SPECIAL operand.

NOSPECIAL
specifies that the user no longer has the SPECIAL attribute.

You must have the SPECIAL attribute to use the NOSPECIAL operand.

TSO | NOTSO
Note: *These operands apply to z/OS systems only.*

TSO
specifies that when you change the profile of a TSO user, you can enter any of the following suboperands to add or change default TSO logon information for that user. Each suboperand defines information that RACF stores in a field within the TSO segment of the user's profile.

You can control access to an entire TSO segment or to individual fields within the TSO segment by using field level access checking. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

ACCTNUM(*account-number*)
specifies the user's default TSO account number when logging on from the TSO/E logon panel. The account number you specify must be defined as a profile in the ACCTNUM general resource class, and the user must be granted READ access to the profile. Otherwise, the user cannot log on to TSO using the specified account number.

Account numbers may consist of any characters, and may be entered with or without single quotation marks. The following rules hold:

- If parentheses, commas, blanks, and semicolons are to be entered as part of the account number, the character string must be enclosed in single quotation marks. For example, if the account number is `(123)`, you must enter `ACCTNUM('(123)')`.
- If a single quotation mark is intended to be part of the account number, and the entire character string is enclosed in single quotation marks, two single quotation marks must be entered together for each single quotation mark within the string. For example, if the account number is `1',` (a one, followed by a single quotation mark, followed by a comma), then you would enter `ACCTNUM('1'',')`. Note that the whole string must be within single quotation marks due to the presence of the comma.
- If the first character of the account number is a single quotation mark, then the string must be entered within single quotation marks and two single quotation marks entered for the first character. For example, if the account number is `'12` (a quote followed by a one, followed by a two), you would enter `ACCTNUM(''12')`.

A user can change an account number, or specify an account number if one has not been specified, using the TSO/E logon panel. RACF checks the user's authorization to the specified account number. If the user is authorized to use the account number, RACF stores the account number in the TSO segment of the user's profile, and TSO/E uses it as a default value the next time the user logs on to TSO/E. Otherwise, RACF denies the use of the account number.

Note that when you define an account number on TSO, you can specify 1 to 40 characters. When you define a TSO account number to RACF, you can specify only 1 to 39 characters.

NOACCTNUM
specifies that you want to delete the user's default account number. If you delete the default account number from a user's profile, RACF uses a default value consistent with current TSO defaults when the user logs on to TSO.

DEST | NODEST

DEST(*destination-id*)
specifies the default destination to which the user can route dynamically allocated SYSOUT data sets. The specified value must be 1 to 7 alphanumeric characters, beginning with an alphabetic or national character.

NODEST
specifies that you want to remove any default destination information for this user. Without explicit action by the user to route SYSOUT, the SYSOUT for this user will be printed at your system default print location.

HOLDCLASS(*hold-class*) | NOHOLDCLASS

HOLDCLASS(*hold-class*)
specifies the user's default hold class. The specified value must be 1 alphanumeric character, excluding national characters.

If you specify the TSO operand on the ALTUSER command but do not specify a value for HOLDCLASS, RACF uses a default value consistent with current TSO defaults.

NOHOLDCLASS
specifies that you want to delete the default hold class from the TSO segment of the user's profile. If you delete the default hold class from a user's profile, RACF uses a default value consistent with current TSO defaults when the user logs onto TSO.

JOBCLASS(*job-class*) | NOJOBCLASS

JOBCLASS(*job-class*)
specifies the user's default job class. The specified value must be 1 alphanumeric character, excluding national characters.

If you specify the TSO operand on the ALTUSER command but do not specify a value for JOBCLASS, RACF uses a default value consistent with current TSO defaults.

NOJOBCLASS
specifies that you want to delete the default job class from the TSO segment of the user's profile. If you delete the default job class from a user's profile, RACF will use a default value consistent with current TSO defaults when the user logs on to TSO.

MAXSIZE(*maximum-region-size*) | NOMAXSIZE

MAXSIZE(*maximum-region-size*)
specifies the maximum region size that the user can request at logon. The maximum region size is the number of 1024-byte units of virtual storage that TSO can create for the user's private address space. The specified value can be an integer in the range of 0 through 65535 for MVS/370 systems, or 0 through 2096128 for MVS/XA or later systems.

If you specify the TSO operand on the ALTUSER command but do not specify a value for MAXSIZE, or specify MAXSIZE(0), RACF uses a default value consistent with current TSO defaults.

Note: This operand is not relevant to z/VM.

NOMAXSIZE
specifies that you want to delete the maximum region size from the TSO segment of the user's profile. If you delete the maximum region size from a user's profile, RACF uses a default value consistent with current TSO defaults when the user logs on to TSO.

MSGCLASS(*message-class*) | NOMSGCLASS

MSGCLASS(*message-class*)
specifies the user's default message class. The specified value must be 1 alphanumeric character, excluding national characters.

If you specify the TSO operand on the ALTUSER command but do not specify a value for MSGCLASS, RACF uses a default value consistent with current TSO defaults.

NOMSGCLASS
specifies that you want to delete the default message class from the TSO segment of the user's profile. If you delete the default message class from a user's profile, RACF uses a default value consistent with current TSO defaults when the user logs on to TSO.

PROC | NOPROC

PROC(*logon-procedure-name*)
specifies the name of the user's default logon procedure when logging on through the TSO/E logon panel. The name you specify must be 1 to 8 alphanumeric characters and begin with an alphabetic character. The name must also be defined as a profile in the TSOPROC general resource class, and the user must be granted READ access to the profile. Otherwise, the user cannot log on to TSO using the specified logon procedure.

A user can change a logon procedure, or specify a logon procedure if one has not been specified, using the TSO/E logon panel. RACF checks the user's authorization to the specified logon procedure. If the user is authorized to use the logon procedure, RACF stores the name of the procedure in the TSO segment of the user's profile, and TSO/E uses it as a default value the next time the user logs on to TSO/E. Otherwise, RACF denies the use of the logon procedure.

NOPROC
specifies that you want to delete the default logon procedure from the TSO segment of the user's profile. If you delete the default logon procedure from a user's profile, RACF uses a default value consistent with current TSO defaults when the user logs on to TSO.

SECLABEL | NOSECLABEL

SECLABEL(*security-label*)
specifies the user's security label if the user specifies one on the TSO logon panel.

NOSECLABEL
specifies that you want to delete the security label from the TSO segment of the user's profile. If you delete the security label from a user's TSO segment, RACF uses the security label in the user's profile the next time the user logs on to TSO.

SIZE | NOSIZE

SIZE(*default-region-size*)
specifies the minimum region size if the user does not request a region size at logon. The default region size is the number of 1024-byte units of virtual storage available in the user's private address space at logon. The specified value can be an integer in the range of 0 through 65535 for MVS/370 systems, or 0 through 2096128 for MVS/XA or later systems.

A user can change a minimum region size, or specify a minimum region size if one has not been specified, using the TSO/E logon panel. RACF stores this value in the TSO segment of the user's profile, and TSO/E uses it as a default value the next time the user logs on to TSO/E.

If you (or a user) specify a value for SIZE that is greater than MAXSIZE, RACF sets SIZE equal to MAXSIZE.

Note: This operand is not relevant to z/VM.

NOSIZE
specifies that you want to delete the default minimum region size from the TSO segment of the user's profile. If you delete the default minimum region size from a user's profile, RACF uses a default value consistent with current TSO defaults when the user logs on to TSO.

SYSOUTCLASS(*sysout-class*) | NOSYSOUTCLASS

SYSOUTCLASS(*sysout-class*)
specifies the user's default SYSOUT class. The specified value must be 1 alphanumeric character, excluding national characters.

If you specify the TSO operand on the ALTUSER command but do not specify a value for SYSOUTCLASS, RACF uses a default value consistent with current TSO defaults.

NOSYSOUTCLASS
specifies that you want to delete the default SYSOUT class from the TSO segment of the user's profile. If you delete the default SYSOUT class from a user's profile, RACF uses a default value consistent with current TSO defaults when the user logs on to TSO.

UNIT | NOUNIT

UNIT(*unit-name*)
specifies the default name of a device or group of devices that a procedure uses for allocations. The specified value must be 1 to 8 alphanumeric characters.

NOUNIT
specifies that you want to delete the default name of a device or group of devices that a procedure uses for allocations from the TSO segment of the user's profile. If you delete this name from a user's profile, RACF uses a default value consistent with current TSO defaults when the user logs on to TSO.

USERDATA | NOUSERDATA

USERDATA(*user-data*)
specifies optional installation data defined for the user. The specified value must be 4 EBCDIC characters; valid characters are 0 through 9 and A through F.

Note: When you change this value for a currently logged-on user ID, the change is overwritten by the TSO logoff command processor when the user ID is logged off.

NOUSERDATA
specifies that you want to delete the installation data previously defined for a user.

NOTSO
specifies that you are revoking a user's authority to use TSO. RACF deletes TSO logon information from the RACF database for the specified user. However, if the user ID is currently logged on, when the user issues the LOGOFF command the TSO logoff processor will restore the TSO segment with default values (except for the USERDATA field which is set to the user's current value). To prevent the TSO segment from being restored, the user ID should be logged off before issuing the ALTUSER NOTSO command.

When you specify NOTSO, the result is the same as if you issue the TSO ACCOUNT command with the DELETE subcommand.

UACC(*access-authority*)
specifies the new default universal access authority for all new resources the user defines while connected to the specified default group. The universal access authorities are ALTER, CONTROL, UPDATE, READ, and NONE. (RACF does not accept EXECUTE access authority with the ALTUSER command.) If you specify UACC without a value, RACF ignores the operand.

This option is group-related. If the user is connected to other groups, the user can have a different default universal access authority in each group.

Note: When an z/OS user (who has the ADSP attribute or specifies the PROTECT parameter on a JCL DD statement) enters the system using the group specified in the GROUP operand as the current connect group, RACF assigns this default universal access authority to any data set or tape volume RACF profiles the user defines.

UAUDIT | NOUAUDIT

UAUDIT
specifies that RACF is to log all RACHECK and RACDEF services issued for the user and all RACF commands (except SEARCH, LISTDSD, LISTGRP, LISTUSER, and RLIST) issued by the user. (When you change a user profile and omit both UAUDIT and NOUAUDIT, the default is NOUAUDIT.)

You must have the AUDITOR attribute, or the user profile must be within the scope of a group in which you have the group-AUDITOR attribute, in order to enter the UAUDIT operand.

NOUAUDIT
specifies that no UAUDIT logging is to be performed. This operand does not override any other auditing options (for example, CMDVIOL specified on SETROPTS) that might be in effect.

You must have the AUDITOR attribute, or the user profile must be within the scope of a group in which you have the group-AUDITOR attribute, to enter the NOUAUDIT operand.

WHEN([DAYS(*day-info*)][TIME(*time-info*)])
specifies the days of the week and/or the hours in the day when the user is allowed to access the system from a terminal. The day-of-week and time restrictions apply only when a user logs on to the system; that is, RACF does not force the user off the system if the end-time occurs while the user is logged on. Also, the day-of-week and time restrictions do not apply to batch jobs; the user can submit a batch job on any day and at any time.

If you specify the WHEN operand, you can restrict the user's access to the system to certain days of the week and to a certain time period within each day. For example, you can restrict a user's access to any one of the following:

- From 9:00 a.m. to 5:00 p.m. (0900:1700); this would be a daily restriction since days were not also specified.
- Monday through Friday; this restriction applies for all 24 hours of Monday, Tuesday, Wednesday, Thursday, and Friday.

- Monday through Friday from 9:00 a.m. to 5:00 p.m. (0900:1700)

Note: You cannot specify more than one combination of days and times, even through multiple ALTUSER commands. For example, if you specify:

```
ALTUSER user_ID WHEN(DAYS(MONDAY TUESDAY) TIME(0100:0500))
ALTUSER user_ID WHEN(DAYS(THURSDAY) TIME(0200:0500))
```

the result is that *user_ID* is allowed to access the system only on Thursday from 2:00 to 5:00; the preceding DAYS (MONDAY TUESDAY) and TIME (0100:0500) operands are overwritten.

To allow a user to access the system only on certain days, specify DAYS(*day-info*), where *day-info* can be any one of the following:

ANYDAY
specifies that the user can access the system on any day.

WEEKDAYS
specifies that the user can access the system only on weekdays (Monday through Friday).

day ...
specifies that the user can access the system only on the days specified, where day can be MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, or SUNDAY, and you can specify the days in any order.

To allow a user to access the system only during a certain time period of each day, specify TIME(*time-info*), where *time-info* can be any one of the following:

ANYTIME
specifies that the user can access the system at any time.

start-time*:*end-time
specifies that the user can access the system only during the specified time period. The format of both *start-time* and *end-time* is hhmm, where hh is the hour in 24-hour notation (00 through 23) and mm is the minutes (00 through 59). Note that 0000 is not a valid time value.

If *start-time* is greater than *end-time*, the interval spans midnight and extends into the following day.

If you omit DAYS and specify TIME, the time restriction applies to any day-of-week restriction already indicated in the profile. If you omit TIME and specify DAYS, the day restriction applies to the time restriction already indicated in the profile. If you specify both DAYS and TIME, the user can access the system only during the specified time period and only on the specified days.

If you omit both DAYS and TIME, the time and day restriction remains as it was in the profile.

WORKATTR | NOWORKATTR
Note: *These operands apply to z/OS systems only.*

WORKATTR
specifies the user-specific attributes of a unit of work.

These operands are used by APPC/MVS for SYSOUT created by APPC transactions.

WAACCNT(*account-number*) | NOWAACCNT
specifies an account number for APPC/MVS processing.

You can specify a maximum of 255 EBCDIC characters. If the value contains any blanks, it must be enclosed in single quotation marks.

NOWAACCNT deletes the account number from the user profile.

WAADDR*n*(*address-line-n*) | NOWAADDR*n*
where *n* can be from 1 to 4, *address-line-n* specifies other address lines for SYSOUT delivery. For each line of the address you can specify a maximum of 60 EBCDIC characters. If an address line contains any blanks, it must be enclosed in single quotation marks.

NOWAADDR*n* deletes address line *n* from the user profile.

WABLDG(*building*) | NOWABLDG
specifies the building that SYSOUT information is to be delivered to.

You can specify a maximum of 60 EBCDIC characters. If the value contains any blanks, it must be enclosed in single quotation marks.

NOWABLDG deletes the building from the profile.

WADEPT(*department*) | NOWADEPT
specifies the department that SYSOUT information is to be delivered to.

You can specify a maximum of 60 EBCDIC characters. If the value contains any blanks, it must be enclosed in single quotation marks.

NOWADEPT deletes the department from the profile.

WANAME(*name*) | NOWANAME
specifies the name of the user SYSOUT information is to be delivered to.

You can specify a maximum of 60 EBCDIC characters. If the value contains any blanks, it must be enclosed in single quotation marks.

NOWANAME deletes the name from the profile.

WAROOM(*room*) | NOWAROOM
specifies the room SYSOUT information is to be delivered to.

You can specify a maximum of 60 EBCDIC characters. If the value contains any blanks, it must be enclosed in single quotation marks.

NOWAROOM deletes the room from the profile.

NOWORKATTR
specifies that you want to delete the work attributes previously defined for a user.

This operand is used by APPC/MVS for SYSOUT created by APPC transactions.

Examples

Example 1

Operation	User IA0 wants to alter the level of group authority from USE to CREATE for user DAF0 in the user's (DAF0's) default group so user DAF0 can define generic profiles for data sets in group RESEARCH.
Known	User IA0 is the owner of user DAF0 and has JOIN authority in the group RESEARCH. The default group for user DAF0 is RESEARCH.
Command	`ALTUSER DAF0 AUTHORITY(CREATE)`
Defaults	GROUP(RESEARCH)

Example 2

Operation	User CD0 wants to correct his name and change his default group to PAYROLL.
Known	The default group for user CD0 is RESEARCH. User CD0 has USE authority in the group PAYROLL.
Command	`ALTUSER CD0 NAME(CDAVIS) DFLTGRP(PAYROLL)`
Defaults	None

Example 3

Operation: User IA0 wants to add the FINANCIAL category and the CONFIDENTIAL security level to user ESH25's profile and restrict the user's access to the system to weekdays from 8:00 A.M. to 8:00 P.M.

Known: User IA0 is connected to group PAYROLL with the group-SPECIAL attribute. Group PAYROLL is user ESH25's default group.

User IA0's profile includes the FINANCIAL category and the CONFIDENTIAL security level. The FINANCIAL category and the CONFIDENTIAL security level have been defined to RACF.

Command:
```
ALTUSER ESH25
ADDCATEGORY(FINANCIAL) SECLEVEL(CONFIDENTIAL)
WHEN(DAYS(WEEKDAYS)TIME(0800:2000))
```

Defaults: None

Example 4

Operation: User RADM02 wants to revoke the user ID of an employee, user D5819, who will be on vacation for three weeks, starting on December 20, 1999.

Known: User RADM02 has the SPECIAL attribute.

Command:
```
ALTUSER D5819 REVOKE(12/20/99) RESUME(1/10/00)
```

Defaults: None

Example 5

Operation: User RGB01 wants to remove all class authorities and the AUDITOR attribute from USER1, and wants to audit all activity by user USER1.

Known: User RGB01 has the SPECIAL and AUDITOR attributes.

User USER1 is an existing user.

Command:
```
ALTUSER USER1 NOCLAUTH(USER TERMINAL) NOAUDITOR
UAUDIT
```

Defaults: None

Example 6

Operation: User RADMIN wants to change the installation-defined information contained in the SJR1 user ID entry, and delete the model name information.

Known: User RADMIN is the owner of user ID SJR1.

Command:
```
ALTUSER SJR1 DATA('RESOURCE USAGE ADMINISTRATOR
NAME TOM P.') NOMODEL
```

Defaults: None

Example 7

Operation A user with SPECIAL authority wants to make existing OpenExtensions user CSMITH a superuser and delete PROGRAM from CSMITH's profile so that the default shell program is used when CSMITH enters the OPENVM SHELL command.

Known User CSMITH is already defined to OVM.

Command
```
ALTUSER CSMITH OVM(UID(0) NOPROGRAM)
```

Defaults None

Example 8

Operation A user with SPECIAL authority wants to change an existing user to a "phrase-only" user by assigning a password phrase and removing the user's current password.

Known User CONRAD is already defined.

Command
```
ALTUSER CONRAD NOPASSWORD PHRASE('Initial
password phrase')
```

Defaults None

Example 9

Operation A user with SPECIAL authority wants to remove all authenticators from a service machine user ID which can only be logged on to using LOGON BY. This prevents the shared user ID from being revoked due to excessive incorrect password, password phrase, and/or MFA attempts.

Known User SERVER1 is already defined.

Command
```
ALTUSER SERVER1 NOPASSWORD NOPHRASE NOMFA
```

Defaults None

Example 10

Operation A help desk consultant wants to reset a user's password.

Known
- The consultant is authorized to reset passwords
- The consultant's RACF user ID (or RACF group associated with the help desk consultant's user ID) has been permitted by the security administrator with READ access to the RACF FACILITY class profile IRR.PASSWORD.RESET.
- The help desk consultant is resetting user JIMBOB's password.

Command
```
ALTUSER JIMBOB PASSWORD(TEMP012X)
```

Defaults EXPIRED

Example 11

Operation A help desk consultant wants to reset an application's password.

Known A help desk consultant has been authorized to reset passwords. The consultant's RACF user ID (or the RACF group associated with the consultant's user ID) has been permitted by the security administrator with UPDATE access to the RACF FACILITY class profile IRR.PASSWORD.RESET

In this example, at the request of operations personnel, the consultant is resetting the user ID associated with an application called CUSTAPP.

The consultant uses the NOEXPIRED operand so the application user ID (CUSTAPP in this example) does not need to change the password when it is logged on.

To reset the application's password, the consultant enters:

Command
```
ALTUSER CUSTAPP PASSWORD(STBR01R) NOEXPIRED
```

Note: The password value STBR01R must satisfy the installation's password quality rules enforced by both SETROPTS and ICHPWX01.

Defaults None.

CONNECT (Connect User to Group)

System environment

This command applies to both z/OS and z/VM systems.

Purpose

Use the CONNECT command to connect a user to a group, modify a user's connection to a group, or assign the group-related user attributes. If you are creating a connection, defaults are available as stated for each operand. If you are modifying an existing connection, no defaults apply.

Note: RACF interprets dates with 2 digit years in the following way, YY represents the 2 digit year.

```
IF 70 < YY <= 99 THEN
   The date is interpreted as 19YY
IF 00 <= YY <= 70 THEN
   The date is interpreted as 20YY
```

Related Commands

- To list a user's connections to a group, use the LISTUSER command as described in "LISTUSER (List User Profile)" on page 179.
- To list the users connected to a group, use the LISTGRP command as described in "LISTGRP (List Group Profile)" on page 172.
- To remove a user from a group, use the REMOVE command as described in "REMOVE (Remove User from Group)" on page 246.

Authorization Required

The specified users and group must already be defined to RACF.

To use the CONNECT command, you must have at least one of the following:

- The SPECIAL attribute
- The group-SPECIAL attribute in the group
- The ownership of the group
- JOIN or CONNECT authority in the group.

You cannot give a user a higher level of authority in the group than you have.

Syntax

The following operands used with the CONNECT command apply to z/OS systems only:

- ADSP | NOADSP
- GRPACC | NOGRPACC

The complete syntax of the command is:

CONNECT CO	(***userid ...***) [AUDITOR | NOAUDITOR] [AUTHORITY(*group-authority*)] [GROUP(*group-name*)] [OPERATIONS | NOOPERATIONS] [OWNER(*userid or group-name*)] [RESUME [(*date*)] | NORESUME] [REVOKE [(*date*)] | NOREVOKE] [SPECIAL | NOSPECIAL] [UACC [(*access-authority*)]]
z/OS Specific Operands:	 [ADSP | NOADSP] [GRPACC | NOGRPACC]

Parameters

userid
specifies the RACF-defined user to be connected to, or modified in, the group specified in the GROUP operand. If you are specifying more than one user, you must enclose the user IDs in parentheses.

For RACF Release 1.7 and earlier releases, the approximate maximum number of users you can connect to one group is 2950. The approximate maximum number of users you can connect to one group is 5900. See *z/VM: RACF Security Server System Programmer's Guide* for information about how to determine the exact maximum number.

This operand is required and must be the first operand following CONNECT.

ADSP | NOADSP
Note: *These operands apply to z/OS systems only.*

ADSP
specifies that when the user is connected to this group, all permanent tape and DASD data sets created by the user will automatically be RACF-protected by discrete profiles.

RACF ignores the ADSP attribute at LOGON/job initiation if SETROPTS NOADSP is in effect.

NOADSP
specifies that the user is not to have the ADSP attribute. If you are creating a connection and omit both ADSP and NOADSP, NOADSP is the default. A user attribute of ADSP specified on the ADDUSER or ALTUSER command overrides NOADSP as a connect attribute.

AUDITOR | NOAUDITOR

AUDITOR
specifies that the user is to have the group-AUDITOR attribute when connected to this group.

To enter the AUDITOR operand, you must have either the SPECIAL attribute or the group-SPECIAL attribute in the group to which you are connecting or modifying the user's profile.

NOAUDITOR
specifies that the user is not to have the group-AUDITOR attribute when connected to this group. When you are creating a connection and omit both AUDITOR and NOAUDITOR, NOAUDITOR is the default. If you are modifying an existing connection, you must have either the SPECIAL attribute or the group-SPECIAL attribute in the group in which you are modifying the user's profile.

A user attribute of AUDITOR specified on the ADDUSER or ALTUSER command overrides NOAUDITOR as a connect attribute.

AUTHORITY(*group-authority*)
specifies the level of authority the user is to have in the group. The valid group authority values are USE, CREATE, CONNECT, and JOIN, as described in "Group Authorities" on page 11. If you are creating a connection and omit AUTHORITY or enter it without a value, the default is USE.

You may not give a user a higher level of authority in the group than you have.

GROUP(*group-name*)
specifies a RACF-defined group. If you omit this operand, the user will be connected to or modified in your current connect group.

Note: RACF allows you to define and connect a user to more than NGROUPS_MAX groups, but when a process is created or OpenExtensions group information is requested, only up to the first NGROUPS_MAX OpenExtensions groups will be associated with the process or user.

The first NGROUPS_MAX OpenExtensions groups to which a user is connected, in alphabetical order, are the groups that get associated with the OpenExtensions user.

See *z/VM: RACF Security Server Macros and Interfaces* for information on NGROUPS_MAX in the ICHNGMAX macro.

GRPACC | NOGRPACC
Note: *These operands apply to z/OS systems only.*

GRPACC
specifies that when the user is connected to this group, any group data sets defined by the user will be automatically accessible to other users in the group. The group whose name is used as the high-level qualifier of the data set name (or the qualifier supplied by a command installation exit) will have UPDATE access authority to the data set.

NOGRPACC
specifies that the user is not to have the GRPACC attribute. If you are creating a connection and omit both GRPACC and NOGRPACC, NOGRPACC is the default. A user attribute of GRPACC specified on the ADDUSER or ALTUSER command overrides NOGRPACC as a connect attribute.

OPERATIONS | NOOPERATIONS

OPERATIONS
specifies that the user is to have the group-OPERATIONS attribute when connected to this group. On z/OS, the group-OPERATIONS user has authorization to do maintenance operations on all RACF-protected DASD data sets, tape volumes, and DASD volumes within the scope of the group unless the access list for a resource specifically limits the OPERATIONS user to an access authority that is less than the operation requires.

On z/VM, the group-OPERATIONS attribute allows the user to access z/VM resources except those where the access list specifically limits the OPERATIONS user to a lower access authority.

You establish the lower access authority for the group-OPERATIONS user through the PERMIT command.

To enter the OPERATIONS operand, you must have the SPECIAL attribute or the group-SPECIAL attribute in the group to which you are connecting or modifying the user's profile.

NOOPERATIONS
specifies that the user is not to have the group-OPERATIONS attribute in this group. If you are creating a connection and omit both OPERATIONS and NOOPERATIONS, NOOPERATIONS is the default. If you are modifying an existing connection, you must have the SPECIAL attribute or the group-SPECIAL attribute in the group in which you are modifying the user's profile.

A user attribute of OPERATIONS specified on the ADDUSER or ALTUSER command overrides NOOPERATIONS as a connect attribute.

OWNER(*userid* or *group-name*)
specifies a RACF-defined user or group to be assigned as the owner of the connect profile. If you are creating a connection and you do not specify an owner, you are defined as the owner of the connect profile.

RESUME | NORESUME

RESUME[(*date*)]
specifies that the user, when connected to the group specified on the GROUP operand, is to be allowed to access the system again. You normally use RESUME to restore access to the system that has been prevented by a prior REVOKE operand. (RESUME, using the current date, is also the default when you are using the CONNECT command to create an initial connection between a user and this group.)

If you specify a date, RACF does not allow the user to access the system until the date you specify. The date must be a future date; if it is not, you are prompted to provide a future date.

During the time between when you specify the RESUME and the date when the RESUME takes effect, the RESUME is called a pending RESUME. You specify a date in the form mm/dd/yy, and you need not specify leading zeros; specifying 9/1/92 is the same as specifying 09/01/92.

If you specify RESUME without a date, the RESUME takes effect immediately. Specifying RESUME without a date overrides any pending RESUME and any pending REVOKE.

When no REVOKE is in effect for the user, RACF ignores the RESUME operand and issues a message.

Note:

1. If you use the ALTUSER command to issue a REVOKE for a user, you must use the ALTUSER command to issue the corresponding RESUME. Issuing RESUME on the CONNECT command does not restore access revoked on the ALTUSER command.
2. If you specify both REVOKE(*date*) and RESUME(*date*), RACF acts on them in date order. For example, if you specify RESUME(8/19/06) and REVOKE(8/5/06), RACF prevents the user from accessing the system from August 5, 2006, to August 18, 2006. On August 19, the user can again access the system.

   If a user is already revoked and you specify RESUME(8/5/06) and REVOKE(8/19/06), RACF allows the user to access the system from August 5, 2006, to August 18, 2006. On August 19, RACF prevents the user from accessing the system.
3. If RACF detects a conflict between REVOKE and RESUME (for example, you specify both without a date), RACF uses REVOKE. If you specify, without a date, only REVOKE or only RESUME, RACF clears both date fields. When RACF revokes a user because of inactivity or invalid password or password phrase attempts, RACF also clears both date fields.
4. To clear the RESUME date field, specify NORESUME.
5. To successfully resume a user whose revoke date has passed, you must specify NOREVOKE to clear the revoke date as well as specifying the RESUME keyword.
6. Downlevel systems sharing the RACF database should not be affected by the changes to REVOKE and RESUME processing.

NORESUME
specifies that RACF is to clear the RESUME date field in the user's group connection. You can use the NORESUME option to cancel the pending resumption (of a user's group connection) that resulted from a previous CONNECT command specified with RESUME(*date*).

REVOKE | NOREVOKE

REVOKE[(*date*)]
specifies that RACF is to prevent the user from accessing the system by attempting to connect to the group specified on the GROUP operand; the user's profile and data sets, however, are not deleted from the RACF database.

If you specify a date, RACF does not prevent the user from accessing the system until the date you specify. The date must be a future date; if it is not, you are prompted to provide a future date.

You specify a date in the form *mm/dd/yy*, where *mm* is the month, *dd* is the day, and *yy* is the year. You need not specify leading zeros; 9/1/06 is the same as 09/01/06. During any time between

when you specify the REVOKE and the date when the REVOKE takes effect, the REVOKE is called a pending revoke.

Note: RACF interprets date fields as:

20*yy* when the year is less than 71
19*yy* when the year is 71 or higher

If you specify REVOKE without a date, the following conditions apply:

- The REVOKE takes effect the next time the user tries to log on to the system.
- Specifying REVOKE without a date overrides any pending REVOKE.

  Note: RESUME works the same way; if you specify RESUME without a date, it also overrides any pending REVOKE.
- Any pending RESUME date remains in effect unless you also specify NORESUME.

  Note: To permanently revoke system access, specify both REVOKE and NORESUME.

When a REVOKE is already in effect for the user, RACF ignores the REVOKE operand and issues a message.

Note:

1. If you specify both REVOKE(*date*) and RESUME(*date*), RACF acts on them in date order. For example, if you specify RESUME(8/19/06) and REVOKE(8/5/06), RACF prevents the user from accessing the system from August 5, 2006, to August 18, 2006. On August 19, the user can again access the system.

   If a user is already revoked and you specify RESUME(8/5/06) and REVOKE(8/19/06), RACF allows the user to access the system from August 5, 2006, to August 18, 2006. On August 19, RACF prevents the user from accessing the system.
2. If RACF detects a conflict between REVOKE and RESUME (for example, you specify both without a date), RACF uses REVOKE. If you specify, without a date, only REVOKE or only RESUME, RACF clears both date fields. When RACF revokes a user because of inactivity or invalid password or password phrase attempts, RACF also clears both date fields.
3. To clear the REVOKE date field, specify NOREVOKE.
4. Downlevel systems sharing the RACF database should not be affected by the changes to REVOKE and RESUME processing.

NOREVOKE
specifies that RACF is to clear the REVOKE date field in the user's group connection. You can use the NOREVOKE option to cancel the pending revocation (of a user's group connection) that resulted from a previous CONNECT command specified with REVOKE(*date*).

To successfully resume a user whose revoke date has passed, you must specify NOREVOKE to clear the revoke date as well as specifying the RESUME keyword.

The NOREVOKE option does not resume the user's group connection after it was revoked by the CONNECT REVOKE command.

SPECIAL | NOSPECIAL

SPECIAL
specifies that the user is to have the group-SPECIAL attribute when connected to this group. To enter the SPECIAL operand, you must have the SPECIAL attribute or the group-SPECIAL attribute in the group to which you are connecting or modifying the user's profile.

NOSPECIAL
specifies that the user is not to have the group-SPECIAL attribute. If you are creating a connection and omit both SPECIAL and NOSPECIAL, NOSPECIAL is the default. If you are modifying an existing connection, you must have the SPECIAL attribute or the group-SPECIAL attribute in the group in which you are modifying the user's profile.

A user attribute of SPECIAL specified on the ADDUSER or ALTUSER command overrides NOSPECIAL as a connect attribute.

UACC[(*access-authority*)]
specifies the default value for the universal access authority for all new resources the user defines while connected to the specified group. The universal access authorities are ALTER, CONTROL, UPDATE, READ, and NONE. (RACF does not accept EXECUTE access authority with the CONNECT command.) If you are creating a connection and omit UACC or enter it without a value, the default is NONE.

This option is group-related. The user can have a different default universal access authority in each of the groups to which the user is connected. When a user (who has the ADSP attribute or specifies the PROTECT parameter on a JCL DD statement) enters the system using the group specified in the GROUP operand as the current connect group, RACF assigns this default universal access authority to any data set or tape volume RACF profiles the user defines.

Examples

Example 1

Operation: User WJE10 wants to connect users AFG5 and GMD2 to group PAYROLL and to make PAYROLL the owner of the connect profiles.

Known: User WJE10 has JOIN authority to group PAYROLL.

User WJE10 is currently connected to group PAYROLL.

Users AFG5 and GMD2 are defined to RACF but not connected to group PAYROLL.

Command:
```
CONNECT (AFG5 GMD2) OWNER(PAYROLL)
```

Defaults: GROUP(PAYROLL) AUTHORITY(USE) UACC(NONE) NOADSP NOGRPACC RESUME NOOPERATIONS NOSPECIAL NOAUDITOR

Example 2

Operation: User WRH0 wants to CONNECT user PDJ6 to group RESEARCH with CREATE authority and universal access of UPDATE.

Known: User WRH0 has CONNECT authority to group RESEARCH.

User WRH0 is not currently connected to group RESEARCH.

User PDJ6 is defined to RACF but is not connected to group RESEARCH.

Command:
```
CONNECT PDJ6 GROUP(RESEARCH) AUTHORITY(CREATE)
UACC(UPDATE)
```

Defaults: NOGRPACC RESUME NOOPERATIONS NOSPECIAL NOAUDITOR NOADSP OWNER(WRH0)

Example 3

Operation: User RADM02 wants to revoke the user ID of an employee, user D5819, who will be on vacation for three weeks, starting on August 5, 1992.

Known: User RADM02 is the owner of the profile for user D5819. Today's date is August 3, 1992.

Command:
```
CONNECT D5819 REVOKE(8/5/92) RESUME(8/26/92)
```

Defaults: None

DELDIR (Delete SFS Directory Profile)

System environment

SFS directories apply to z/VM systems only.

Purpose

Use the DELDIR command to delete either a discrete or generic directory profile from the RACF database. (Note that the SFS directory itself is not physically deleted.)

Related Commands

- To protect an SFS directory with a discrete or generic profile, use the ADDDIR command as described in "ADDDIR (Add SFS Directory Profile)" on page 16.
- To change an SFS directory profile, use the ALTDIR command as described in "ALTDIR (Alter SFS Directory Profile)" on page 66.
- To list the information in the SFS directory profiles, use the LDIRECT command as described in "LDIRECT (List SFS Directory Profile)" on page 148.
- To permit or deny access to an SFS directory profile, use the PERMDIR command as described in "PERMDIR (Maintain SFS Directory Access Lists)" on page 194.
- To obtain a list of SFS directory profiles, use the SRDIR command as described in "SRDIR (Obtain a List of SFS Directory Profiles)" on page 324.

Authorization Required

To delete a discrete or generic directory profile, you must have sufficient authority over the directory. RACF performs authorization checking in the following sequence until you meet one of these conditions:

- You have the SPECIAL attribute.
- The directory profile is within the scope of a group in which you have the group-SPECIAL attribute.
- The userid qualifier of the profile name is your user ID.
- You are the owner of the profile.

For discrete profiles only:

- The directory is protected by a discrete profile and you are on the access list with ALTER authority.
- The directory is protected by a discrete profile and your group or one of your groups (if list of groups checking is active) is on the access list and has ALTER authority.
- The directory is protected by a discrete profile and the universal access authority is ALTER.

Syntax

The complete syntax of the DELDIR command is:

```
DELDIR                profile-name
DDIR
```

Parameters

profile-name

specifies the name of the existing discrete or generic profile to be deleted from the RACF database. You may specify only one profile. For the format of these profile names, see "Profile Names for SFS Files and Directories" on page 342.

This operand is required.

Examples

Example

Operation: User SMITH wants to remove RACF protection from his PROJECT directory

Known: The file pool ID is POOL1.

Command:
```
DELDIR POOL1:SMITH.PROJECT
```

Defaults: None

DELDSD (Delete Data Set Profile)

System environment

Data sets apply to z/OS systems only.

Purpose

Use the DELDSD command to remove RACF protection from tape or DASD data sets that are protected by either discrete or generic profiles.

When RACF-protection is removed from a data set protected by a discrete profile:

- The RACF indicator for the data set is turned off. For a DASD data set, the indicator is in the DSCB for a non-VSAM data set or in the catalog entry for a VSAM data set. For a tape data set, the indicator is in the TVTOC entry for the data set in the corresponding TAPEVOL profile.
- The data set profile is deleted from the RACF database. (Note that the data set itself is not physically deleted or scratched.)

  If all the datasets in the TVTOC have expired, then RACF deletes the TAPEVOL profiles and the associated tape DATASET profiles.

To remove RACF protection from a non-VSAM DASD data set that is protected by a discrete profile, the data set must be online and not currently in use. For a VSAM data set that is protected by a discrete profile, the catalog for the data set must be online. The VSAM data set itself must also be online if the VSAM catalog recovery option is being used. If the required data set or catalog is not online, the DELDSD command processor will, if you have the TSO MOUNT authority, request that the volume be mounted.

Changes made to discrete profiles take effect after the DELDSD command is processed. Changes made to generic profiles do not take effect until one or more of the following steps is taken:

- The user of the data set issues the LISTDSD command:

  ```
  LISTDSD DA(data-set-protected-by-the-profile) GENERIC
  ```

  Note: Use the data set name, not the profile name.
- The security administrator issues the SETROPTS command:

  ```
  SETROPTS GENERIC(DATASET) REFRESH
  ```

  See SETROPTS command for authorization requirements.
- The user of the data set logs off and logs on again.

For more information, refer to *z/VM: RACF Security Server Security Administrator's Guide*.

Related Commands

- To create a data set profile, use the ADDSD command as described in “ADDSD (Add Data Set Profile)” on page 33.
- To change a data set profile, use the ALTDSD command as described in “ALTDSD (Alter Data Set Profile)” on page 71.
- To display a data set profile, use the LISTDSD command as described in “LISTDSD (List Data Set Profile)” on page 160.

Authorization Required

To remove RACF protection from a data set or to delete a generic data set profile, you must have sufficient authority over the data set. RACF performs authorization checking in the following sequence until you meet one of these conditions:

- You have the SPECIAL attribute
- The data set profile is within the scope of a group in which you have the group-SPECIAL attribute
- The high-level qualifier of the profile name (or the qualifier supplied by a command installation exit) is your user ID
- You are the owner of the profile.

For discrete profiles only:

- The data set is protected by a discrete profile, and you are on the access list with ALTER authority
- The data set is protected by a discrete profile, and your group or one of your groups (if checking list of groups is active) is on the access list and has ALTER authority
- The data set is protected by a discrete profile, and the universal access authority is ALTER.

Syntax

The complete syntax of the DELDSD command is:

```
DELDSD          (profile-name ...)
DD              [ GENERIC | NOSET | SET ]
                [ VOLUME(volume-serial) ]
```

Note: If you specify a generic profile name, RACF ignores the VOLUME, SET, and NOSET operands.

Parameters

profile-name ...
specifies the name of the discrete or generic profile. If you specify more than one profile, the list must be enclosed in parentheses.

This operand is required and must be the first operand following DELDSD.

Note: Because RACF uses the RACF database and not the system catalog, you cannot use alias data set names.

GENERIC | NOSET | SET

GENERIC
specifies that RACF is to treat the profile name as a generic name, even if it does not contain any generic characters.

NOSET | SET
specifies whether the RACF indicator should be set off or not.

If the profile name contains a generic character or if you specify GENERIC, RACF ignores this operand.

NOSET
specifies that RACF is not to turn off the RACF indicator for the data set.

Use NOSET when you are transferring a RACF-indicated data set to another system where it is also to be RACF-protected. Leaving the indicator on prevents unauthorized access to the data set until it can be redefined on the new system. (To delete multiple data set profiles, see Example 2 for the SEARCH command.)

When you specify NOSET for a tape data set protected by a discrete profile, RACF deletes the discrete profile but retains the TVTOC entry for the data set name. You can then use a generic profile to protect the data set.

If you specify NOSET, the volumes on which the data set or catalog resides need not be online.

To use NOSET, you must have the SPECIAL attribute, the data set profile must be within the scope of a group in which you have the group-SPECIAL attribute, or the high-level qualifier of the data set name (or the qualifier supplied by the naming conventions table or by a command installation exit) must be your user ID.

SET
specifies that RACF is to turn off the RACF indicator for the data set. Use SET, which is the default value, when you are removing RACF protection for a data set. If the indicator is already off, the command fails.

You cannot delete discrete profiles using SET with RACF z/VM.

VOLUME(*volume-serial*)
specifies the volume on which the tape data set, the non-VSAM DASD data set, or the catalog for the VSAM data set resides.

If you specify this operand and *volume-serial* does not appear in the profile for the data set, the command fails.

If the data set name appears more than once in the RACF database and you do not specify VOLUME, the command fails. If the data set name appears only once and you do not specify VOLUME, no volume serial number checking is performed, and processing continues.

If the profile name contains a generic character or if you specify GENERIC, RACF ignores this operand.

Examples

Example 1

Operation	User EH0 wants to remove discrete profile RACF protection from data set CD0.DEPT1.DATA.
Known	User EH0 owns data set CD0.DEPT1.DATA.
Command	`DELDSD 'CD0.DEPT1.DATA'`
Defaults	SET

Example 2

Operation	User KLE05 wants to remove discrete profile protection from data set KLE05.DUPDS1.DATA. The data set is a duplicate data set, and the user wants to remove the profile for the data set on volume DU2 without turning off the RACF indicator.
Command	`DELDSD DUPDS1.DATA VOLUME(DU2) NOSET`
Defaults	None

Example 3

Operation	User KLE05 wants to delete the generic profile and remove RACF protection from the data set or sets protected by the profile SALES.*.DATA
Known	User KLE05 has the group-SPECIAL attribute in group SALES.
Command	`DELDSD 'SALES.*.DATA'`
Defaults	None

DELFILE (Delete SFS File Profile)

System environment

SFS files apply to z/VM systems only.

Purpose

Use the DELFILE command to delete either a discrete or generic file profile from the RACF database. (Note that the file itself is not physically deleted or scratched.)

Related Commands

- To protect an SFS file with a discrete or generic profile, use the ADDFILE command as described in "ADDFILE (Add SFS File Profile)" on page 22.
- To change an SFS file, use the ALTFILE command as described in "ALTFILE (Alter SFS File Profile)" on page 81.
- To list the information in the SFS file profile(s), use the LFILE command as described in "LFILE (List SFS File Profile)" on page 154.
- To permit or deny access to an SFS file, use the PERMFILE command as described in "PERMFILE (Maintain SFS File Access Lists)" on page 198.
- To obtain a list of SFS file profiles, use the SRFILE command as described in "SRFILE (Obtain a List of SFS File Profiles)" on page 329.

Authorization Required

To delete a discrete or generic file profile, you must have sufficient authority over the file. RACF performs authorization checking in the following sequence until you meet one of these conditions:

- You have the SPECIAL attribute.
- The file profile is within the scope of a group in which you have the group-SPECIAL attribute.
- The user ID qualifier of the profile name is your user ID.
- You are the owner of the profile.

For discrete profiles only:

- The file is protected by a discrete profile and you are on the access list with ALTER authority.
- The file is protected by a discrete profile and your group or one of your groups (if list of groups checking is active) is on the access list and has ALTER authority.
- The file is protected by a discrete profile and the universal access authority is ALTER.

Syntax

The complete syntax of the DELFILE command is:

```
DELFILE              profile-name
DF
```

Parameters

profile-name
specifies the name of the discrete or generic profile to be deleted from the RACF database. You may specify only one *profile-name*. For the format of these profile names, see "Profile Names for SFS Files and Directories" on page 342.

This value is required.

Examples

Example 1

Operation	User SFSADM1 wants to remove RACF protection from all of user JIM's files which are protected by the profile * * POOL1:JIM.**.
Known	SFSADM1 has the SPECIAL attribute.
Command	`DELFILE * * POOL1:JIM.**`
Defaults	none

Example 2

Operation	User SMITH wants to remove RACF protection from his PROJECT SCRIPT file.
Known	SMITH's file pool is POOL1.
Command	`DELFILE PROJECT SCRIPT POOL1:SMITH.`
Defaults	none

DELGROUP (Delete Group Profile)

System environment

This command applies to both z/OS and z/VM systems.

Purpose

Use the DELGROUP command to delete a group and its relationship to its superior group from RACF.

There are, however, other places in the RACF database where the group name may appear, and DELGROUP processing does not delete these other occurrences of the group name. For example, the group name could be in the access list for any resource. You can use the RACF cross reference utility (IRRUT100) program to find any occurrences of the group name in the RACF database. (See *z/VM: RACF Security Server System Programmer's Guide* for a description of this utility.) Then use the PERMIT command to remove the group name from any access list where it exists.

Related Commands

- To add a group profile to the RACF database, use the ADDGROUP command as described in "ADDGROUP (Add Group Profile)" on page 28.
- To change a group profile in the RACF database, use the ALTGRP command as described in "ALTGROUP (Alter Group Profile)" on page 86.
- To connect a user to a group, use the CONNECT command as described in "CONNECT (Connect User to Group)" on page 128.
- To list information related to a group profile, use the LISTGRP command as described in "LISTGRP (List Group Profile)" on page 172.
- To remove a user from a group profile, use the REMOVE command as described in "REMOVE (Remove User from Group)" on page 246.

Authorization Required

To use the DELGROUP command, at least one of the following must be true:

- You must have the SPECIAL attribute
- The group to be deleted must be within the scope of a group in which you have the group-SPECIAL attribute
- You must be the owner of the superior group
- You must have JOIN authority in the superior group
- You must be the owner of the group to be deleted.

Syntax

The complete syntax of the DELGROUP command is:

```
DELGROUP                (group-name ...)
DG
```

Parameters

group-name
specifies the name of the group whose profile is to be removed from the RACF database. If you are deleting more than one group, you must enclose the list of group names in parentheses.

You must enter at least one group name. For each group name you enter, the following conditions must exist:

- The group must be defined to RACF.
- The group must not have any subgroups.
- The group must not have any group data sets (data sets whose names are qualified by the group name or begin with the value supplied by an installation exit).
- The group must not have any users connected to it.

Examples

Example

Operation: User WJE10 wants to delete subgroups DEPT1 and DEPT2 from group PAYROLL.

Known: User WJE10 has JOIN authority to group PAYROLL.

DEPT1 and DEPT2 are subgroups of group PAYROLL.

Neither DEPT1 nor DEPT2 have any subgroups or users connected to them. In addition, neither group has any group data sets.

Command:
```
DELGROUP (DEPT1 DEPT2)
```

Defaults: None

DELUSER (Delete User Profile)

System environment

This command applies to both z/OS and z/VM systems.

Purpose

Use the DELUSER command to delete a user from RACF.

This command removes the user's profile and all user-to-group connections for the user. (The connect profiles define the user's connections to various RACF groups.)

There are, however, other places in the RACF database where the user's user ID might appear, and the DELUSER command does not delete the user ID from all these places. Specifically, the user could be the owner of a group, the owner of a user's profile, the owner of a group data set, or in an access list for any resource. Before issuing DELUSER, you must first issue the REMOVE command to assign new owners for any group data sets the user owns in groups other than his default group. You can use the RACF cross reference utility program (IRRUT100) to find any other occurrences of the user ID. (See *z/VM: RACF Security Server System Programmer's Guide* for a description of this utility.) Then use the ALTGROUP, ALTUSER, ALTDSD, RALTER, and PERMIT commands, as required, to change ownerships and remove access authorities.

If the user is logged on, the user will remain active until logging off. Therefore, you might consider having the operator examine any logons that are active for the user and FORCE those that should not be allowed to continue.

Related Commands

- To add a user profile to the RACF database, use the ADDUSER command as described in "ADDUSER (Add User Profile)" on page 45.
- To change a user profile in the RACF database, use the ALTUSER command as described in "ALTUSER (Alter User Profile)" on page 93.
- To list information in a user profile, use the LISTUSER command as described in "LISTUSER (List User Profile)" on page 179.

Authorization Required

To use the DELUSER command, at least one of the following must be true:

- You must have the SPECIAL attribute
- The user profile to be deleted must be within the scope of a group in which you have the group-SPECIAL attribute
- You must be the owner of the user's profile.

Note: JOIN authority in the user's default group is not sufficient authority to delete the user from RACF.

Syntax

The complete syntax of the DELUSER command is:

```
DELUSER                (userid ...  )
DU
```

Parameters

userid
specifies the user ID of the user whose profile is to be deleted from the RACF database. If you are deleting more than one user, you must enclose the list of user IDs in parentheses. You must enter at least one user ID. For each user ID you enter, the following conditions must exist:

- The user must be defined to RACF
- The z/OS user must not have any user data sets defined to RACF. (User data sets are data sets whose names are qualified by the user ID of the user being deleted or begin with the value supplied by an installation exit.)

Examples

Example

Operation: User WJE10 wants to delete user AEH0 from RACF.

Known: User AEH0 is defined to RACF.

User AEH0 is not the owner of any RACF profiles.

User WJE10 is connected to group PAYROLL (and is the owner of user AEH0) with the group-SPECIAL attribute.

Command:
```
DELUSER  AEH0
```

Defaults: None

END (End RACF Command Session on z/VM)

System environment

This command applies to z/VM systems only.

Purpose

Use the END command to terminate a RACF command session on z/VM.

Related Commands

To start a RACF command session, use the RACF command (z/VM only) as described on page "RACF (Begin RACF Command Session on z/VM)" on page 211.

Authorization Required

Any user who can enter a RACF command session can use the END command.

Syntax

The complete syntax of the END command is:

```
END
```

HELP (Obtain RACF Help)

System environment

This command applies to both z/OS and z/VM systems.

Purpose

Use the HELP command to obtain information about the function, syntax, and operands of RACF commands as well as information about certain messages that can appear during a RACF command session. This information is displayed at your terminal in response to your request for help.

Authorization Required

You need no special attribute or authority to use the HELP command. Any user who can log on to z/VM can issue this command.

Syntax

The complete syntax of the HELP command is:

```
HELP                [ command-name ]
H                   [ ALL ]
                    [ FUNCTION ]
                    [ OPERANDS [(operand...)] ]
                    [ SYNTAX ]
```

Parameters

command-name
specifies the name of the command about which you want information.

If you specify this operand, it must be the first operand following HELP.

If you are in a RACF command session and omit this operand, you will obtain a list of all the RACF commands and their respective functions.

Note: For more information about z/VM systems, see "Getting Online HELP" in “Choosing between Using RACF Commands and ISPF Panels” on page 7.

ALL
specifies that you want to see all the available information about the command. This information includes the function, syntax, and operands of the command. If no other keyword operand is specified, ALL is the default value.

FUNCTION
specifies that you want to see information about the purpose and operation of the command.

OPERANDS[(*operand*...)]
specifies that you want to see information about the operands of the command. When you specify OPERANDS and omit any values, all operands for the command will be described. To obtain information about a particular operand, specify that operand within parentheses following OPERANDS. If you specify more than one operand, separate the operand names by either commas or blanks.

SYNTAX
specifies that you want to see information about the proper syntax of the command.

Examples

Example 1

Operation: User LQJ0 wants to see all available information for the ADDUSER command.

Known: User LQJ0 is RACF-defined.

Command:
```
HELP ADDUSER
```

Defaults: ALL

Example 2

Operation: User JXN01 wants to see a description of the AUDIT, ADDMEM, DATA, and SECLEVEL operands for the RDEFINE command.

Known: User JXN01 is RACF-defined.

Command:
```
HELP RDEFINE OPERANDS(AUDIT ADDMEM DATA
SECLEVEL)
```

Defaults: None

Example 3

Operation: User MJW02 wants to see a description of the function and syntax of the SETROPTS command.

Known: User MJW02 is RACF-defined.

Command:
```
HELP SETROPTS FUNCTION SYNTAX
```

Defaults: None

HELP Example for z/VM (RAC Command Processor):

Example 4

Operation: User LQJ0 wants to see all available information for the ADDUSER command.

Known: User LQJ0 is RACF-defined.

Command:
```
RAC HELP ADDUSER
```

Defaults: ALL

LDIRECT (List SFS Directory Profile)

System environment

SFS directories apply to z/VM systems only.

Purpose

Use the LDIRECT command to list information included in directory profiles.

You can request the details for a specific profile by giving the full name of the profile. You can also request the details for all profiles for which you have the proper authority.

Profiles are listed in alphabetic order. Generic profiles are listed in the same order as they are searched for a resource match.

Note: RACF interprets dates with 2 digit years in the following way, YY represents the 2 digit year.

```
IF 70 < YY <= 99 THEN
   The date is interpreted as 19YY
IF 00 <= YY <= 70 THEN
   The date is interpreted as 20YY
```

The details RACF lists from each directory profile are:

- The level
- The owner
- The type of access attempts (as specified by the AUDIT operand on the ADDDIR or ALTDIR command) that are being logged on the SMF data file
- The universal access authority
- Your highest level of access authority
- The user, if any, to be notified when RACF uses this profile to deny access to a resource
- The type of access attempts (as specified by the GLOBALAUDIT operand on the ALTDIR command) that are being logged on the SMF data file (for auditors only)
- Installation-defined data as specified on the DATA operand of the ADDDIR or ALTDIR command

  Note: If your installation is configured to be a B1 security environment, this information will not be listed in your output. * SUPPRESSED * will appear under the installation data field. Only those with system SPECIAL will be allowed to list the field.
- Application-defined data as specified on the APPLDATA operand of the ADDDIR or ALTDIR command

  Note: If your installation is configured to be a B1 security environment, this information will not be listed in your output. * SUPPRESSED * will appear under the application data field. Only those with system SPECIAL will be allowed to list the field.
- The status of the WARNING|NOWARNING indicator

Additional details:

You can request the following details by using the appropriate LDIRECT operands:

- The security label, the security level and categories

  (see the AUTHUSER operand)
- The number of times the directory was accessed by all users for each of the following access authorities[1]

[1] This detail is only meaningful when your installation is gathering resource statistics. For a generic profile, RACF replaces any statistics line with NOT APPLICABLE FOR GENERIC PROFILE.

ALTER, CONTROL, UPDATE, READ

(See the STATISTICS operand)

- Historical data, such as:
  - Date the directory was defined to RACF
  - Date the directory was last referenced [1]
  - Date the directory was last updated [1]

  (see the HISTORY operand)
- The standard access list, which displays:
  - All users and groups authorized to access the directory
  - The level of authority for each user and group
  - The number of times each user has accessed the directory [1]

  (see the AUTHUSER operand)
- The conditional access list, which displays the same fields as the standard access list, as well as the following additional fields:
  - The class of the resource
  - The entity name of the resource

Related Commands

- To protect an SFS directory with a discrete or generic profile, use the ADDDIR command as described in "ADDDIR (Add SFS Directory Profile)" on page 16.
- To change an SFS directory profile, use the ALTDIR command as described in "ALTDIR (Alter SFS Directory Profile)" on page 66.
- To delete an SFS directory profile, use the DELDIR command as described in "DELDIR (Delete SFS Directory Profile)" on page 134.
- To permit or deny access to an SFS directory profile, use the PERMDIR command as described in "PERMDIR (Maintain SFS Directory Access Lists)" on page 194.
- To obtain a list of SFS directory profiles, use the SRDIR command as described in "SRDIR (Obtain a List of SFS Directory Profiles)" on page 324.

Authorization Required

To list the details of a directory profile, you must have a sufficient level of authority for each profile listed as the result of your request. RACF makes the following checks for each profile until one of the conditions is met:

- You have the SPECIAL attribute.
- The profile is within the scope of a group in which you have the group-SPECIAL attribute.
- You have the OPERATIONS attribute.
- The profile is within the scope of a group in which you have the group-OPERATIONS attribute.
- You have the AUDITOR or ROAUDIT attribute.
- The directory profile is within the scope of a group in which you have the group-AUDITOR attribute.
- The userid qualifier of the directory name is your user ID.
- You are the owner of the directory.
- You are on the profile's access list with at least READ authority. (If your level of authority is NONE, the directory is not listed.)

- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is in the access list and has at least READ authority. (If the level of authority for any group that RACF checked is NONE, the directory is not listed.)
- The universal access authority is at least READ.
- You have at least READ authority from the global access checking table (if this table contains an entry for the profile).

You will see the type of access attempts, as specified by the GLOBALAUDIT operand, only if you have the AUDITOR attribute or the profile is within the scope of a group in which you have the group-AUDITOR attribute.

AUTHUSER Conditions

When you specify the AUTHUSER operand to display the access list for a profile, RACF checks your level of authority for each profile until one of the following conditions is met:

- You have the SPECIAL attribute.
- The profile is within the scope of a group in which you have the group-SPECIAL attribute.
- You have the OPERATIONS attribute.
- The profile is within the scope of a group in which you have the group-OPERATIONS attribute.
- The userid qualifier of the directory name is your user ID.
- You are the owner of the directory.
- You have the AUDITOR or ROAUDIT attribute.
- The directory profile is within the scope of a group in which you have the group-AUDITOR attribute.
- You have ALTER authority from the global access checking table (if this table contains an entry for the profile).

For discrete profiles only:

- You are on the profile's access list with ALTER authority. (If you have any other level of authority, you may not use the operand.)
- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is in the access list and has ALTER authority. (If any group that RACF checked has any other level of authority, you may not use the operand.)
- The universal access authority is ALTER.

Syntax

The complete syntax of the LDIRECT command is:

```
LDIRECT              {profile-name | *}
LDIR                 [ ALL ]
                     [ AUTHUSER   ]
                     [ {GENERIC | NOGENERIC} ]
                     [ HISTORY    ]
                     [ STATISTICS ]
```

Note: This command is an extension of the RLIST command as it applies to the DIRECTRY class. Other RLIST parameters, such as SESSION and DLFDATA are also accepted on the command, but are not listed here. If they are specified on this command, they will be processed as on RLIST, but they have no meaning for SFS.

Parameters

***profile-name* | ***

profile-name
specifies the name of the discrete or generic profile about which information is to be displayed. You may specify only one profile and the name must be in SFS format. For the format of these profile names, see "Profile Names for SFS Files and Directories" on page 342.

This operand or * is required.

***
an asterisk (*) specifies that you want to display information for all directories for which you have proper authority.

ALL
specifies that you want all information for each directory profile displayed.

The access list is not included unless you have sufficient authority to use the AUTHUSER operand, as described in "Authorization Required" on page 149. The list does not include the type of access attempts (as specified by the GLOBALAUDIT operand on the ALTDIR command) that are being logged on the SMF data file unless you have the AUDITOR or group-AUDITOR attribute.

AUTHUSER
specifies that you want to see the access list for each profile. The output shows the following:

- The user categories authorized to access the resource
- The security level required to access the resource
- The security label required to access the resource
- The standard access list. This includes the following:
  - All users and groups authorized to access the resource
  - The level of authority for each user and group
  - The number of times the user has accessed the resource[2]
- The conditional access list. This list consists of the same fields as in the standard access list, as well as the following fields:
  - The class of the resource via which each user and group in the list can access the target resource of the command. For example, if a user can access the target resource via terminal TERM01, then TERMINAL would be the class listed.
  - The entity name of the resource via which each user and group in the list can access the target resource of the command. In the example above, TERM01 would be listed.

You must have sufficient authorization to use the AUTHUSER operand, as described in "Authorization Required" on page 149.

GENERIC | NOGENERIC

GENERIC
specifies that you want RACF to display information for the generic profile that most closely matches an SFS directory name. If you specify GENERIC, RACF ignores a discrete profile that protects the SFS directory. If asterisk (*) is specified instead of the profile name, all generic directory profiles will be listed.

NOGENERIC
specifies that you want RACF to display information for the discrete profile that protects an SFS directory. If asterisk (*) is specified instead of the profile name, all discrete directory profiles will be listed.

[2] This detail is only meaningful when your installation is gathering resource statistics. For a generic profile, RACF replaces any statistics line with NOT APPLICABLE FOR GENERIC PROFILE.

If neither GENERIC nor NOGENERIC is specified, RACF lists information for the discrete directory name that matches the directory name you specify. If there is no matching discrete profile, RACF will list the generic profile that most closely matches the directory name. If asterisk (*) is specified instead of the profile name, all discrete and generic profiles will be listed.

Assume the following profiles exist in the DIRECTRY class:

```
FP:LAURIE.DIR1
FP:LAURIE.DIR%        (G)
FP:LAURIE.**          (G)
FP:LAURIE.DIR1.DIR2
```

- If you enter

  ```
  LDIRECT FP:LAURIE.DIR1 GENERIC
  ```

  RACF will list profile FP:LAURIE.DIR% (best matching generic profile)
- If you enter

  ```
  LDIRECT FP:LAURIE.DIR1
  ```

  RACF will list profile FP:LAURIE.DIR1 (discrete profile found first)
- If you enter

  ```
  LDIRECT FP:LAURIE.DIR4.DIR5 NOGENERIC
  ```

  RACF will not list any profiles, because no matching discrete profile exists (even though a matching generic does exist, FP:LAURIE.**)

HISTORY

specifies that you want to list the following data:

- Date each profile was defined to RACF
- Date each directory was last referenced [3]
- Date of last RACROUTE REQUEST=AUTH for UPDATE authority. [3]

STATISTICS

specifies that you want to list the statistics for each profile. The list includes the number of times the profile was accessed by users with READ, UPDATE, CONTROL and ALTER authorities, as well as a separate total for each authority level. [3]

Examples

Example

Operation	User GARY wants to list all information for his DIR1.DIR2 directory.
Known	User GARY is RACF-defined and does not have the AUDITOR attribute.
Command	`LDIRECT FP1:GARY.DIR1.DIR2 ALL`
Defaults	None
Output	See Figure 2 on page 153

[3] This detail is only meaningful when your installation is gathering resource statistics. For a generic profile, RACF replaces any statistics line with NOT APPLICABLE FOR GENERIC PROFILE.

```
LDIRECT FP1:GARY.DIR1.DIR2

    CLASS       NAME
    -----       ----
    DIRECTRY    FP1:GARY.DIR1.DIR2

    LEVEL  OWNER    UNIVERSAL ACCESS  YOUR ACCESS   WARNING
    -----  -------- ----------------  -----------   -------
     00    GARY           NONE             ALTER     NO

    INSTALLATION DATA
    -----------------
    NONE

    APPLICATION DATA
    -----------------
    NONE

    SECLEVEL
    --------
    NO SECLEVEL

    CATEGORIES
    ----------
    NO CATEGORIES

    SECLABEL
    ----------
    NO SECLABEL

    AUDITING
    --------
    FAILURES(READ)

    NOTIFY
    --------
    NO USER TO BE NOTIFIED

    CREATION DATE  LAST REFERENCE DATE  LAST CHANGE DATE
     (DAY) (YEAR)       (DAY) (YEAR)      (DAY) (YEAR)
    -------------  -------------------  ----------------
      071    95          076    95         076    95

    ALTER COUNT   CONTROL COUNT   UPDATE COUNT   READ COUNT
    -----------   -------------   ------------   ----------
      000000         000000         000000         000000

    USER      ACCESS   ACCESS COUNT
    ----      ------   ------ -----
    GARY      ALTER       000000

    NO ENTRIES IN CONDITIONAL ACCESS LIST
```

Figure 2. Example 1. Output for LDIRECT Command

LFILE (List SFS File Profile)

System environment

SFS files apply to z/VM systems only.

Purpose

Use the LFILE command to list information included in file profiles.

You can request the details for a specific profile by giving the full name of the profile. You can also request the details for all profiles for which you have the proper authority.

Profiles are listed in alphabetic order. Generic profiles are listed in the same order as they are searched for a resource match.

Note: RACF interprets with 2 digit years in the following way, YY represents the 2 digit year.

```
IF 70 < YY <= 99 THEN
   The date is interpreted as 19YY
IF 00 <= YY <= 70 THEN
   The date is interpreted as 20YY
```

The details RACF lists from each file profile are:

- The level
- The owner
- The type of access attempts (as specified by the AUDIT operand on the ADDFILE or ALTFILE command) that are being logged on the SMF data file
- The universal access authority
- Your highest level of access authority
- The user, if any, to be notified when RACF uses this profile to deny access to a resource
- The type of access attempts (as specified by the GLOBALAUDIT operand on the ALTFILE command) that are being logged on the SMF data file (for auditors only)
- Installation-defined data as specified on the DATA operand of the ADDFILE or ALTFILE command

  Note: If your installation is configured to be a B1 security environment, this information will not be listed in your output. * SUPPRESSED * will appear under the installation data field. Only those with system SPECIAL will be allowed to list the field.
- Application-defined data as specified on the APPLDATA operand of the ADDFILE or ALTFILE command

  Note: If your installation is configured to be a B1 security environment, this information will not be listed in your output. * SUPPRESSED * will appear under the application data field. Only those with system SPECIAL will be allowed to list the field.
- The status of the WARNING|NOWARNING indicator

Additional details:

You can request the following details by using the appropriate LFILE operands:

- The security label, the security level and categories

  (see the AUTHUSER operand)
- The number of times the file was accessed by all users for each of the following access authorities[4]

[4] This detail is only meaningful when your installation is gathering resource statistics. For a generic profile, RACF replaces any statistics line with NOT APPLICABLE FOR GENERIC PROFILE.

ALTER, CONTROL, UPDATE, READ

(See the STATISTICS operand)

- Historical data, such as:
  - Date the file was defined to RACF
  - Date the file was last referenced [4]
  - Date the file was last updated [4]

  (see the HISTORY operand)
- The standard access list, which displays:
  - All users and groups authorized to access the file
  - The level of authority for each user and group
  - The number of times each user has accessed the file [4]

  (see the AUTHUSER operand)
- The conditional access list, which displays the same fields as the standard access list, as well as the following additional fields:
  - The class of the resource
  - The entity name of the resource

Related Commands

- To protect an SFS file with a discrete or generic profile, use the ADDFILE command as described in "ADDFILE (Add SFS File Profile)" on page 22.
- To change an SFS file profile, use the ALTFILE command as described in "ALTFILE (Alter SFS File Profile)" on page 81.
- To delete an SFS file profile, use the DELFILE command as described in "DELFILE (Delete SFS File Profile)" on page 139.
- To permit or deny access to an SFS file, use the PERMFILE command as described in "PERMFILE (Maintain SFS File Access Lists)" on page 198.
- To obtain a list of SFS file profiles, use the SRFILE command as described in "SRFILE (Obtain a List of SFS File Profiles)" on page 329.

Authorization Required

To list the details of a file profile, you must have a sufficient level of authority for each profile listed as the result of your request. RACF makes the following checks for each profile until one of the conditions is met:

- You have the SPECIAL attribute.
- The profile is within the scope of a group in which you have the group-SPECIAL attribute.
- You have the OPERATIONS attribute.
- The profile is within the scope of a group in which you have the group-OPERATIONS attribute.
- You have the AUDITOR or ROAUDIT attribute.
- The file profile is within the scope of a group in which you have the group-AUDITOR attribute.
- The userid qualifier of the file name is your user ID.
- You are the owner of the file.
- You are on the profile's access list with at least READ authority. (If your level of authority is NONE, the file is not listed.)

- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is in the access list and has at least READ authority. (If the level of authority for any group that RACF checked is NONE, the file is not listed.)
- The universal access authority is at least READ.
- You have at least READ authority from the global access checking table (if this table contains an entry for the profile).

You will see the type of access attempts, as specified by the GLOBALAUDIT operand, only if you have the AUDITOR attribute or the profile is within the scope of a group in which you have the group-AUDITOR attribute.

AUTHUSER Conditions

When you specify the AUTHUSER operand to display the access list for a profile, RACF checks your level of authority for each profile until one of the following conditions is met:

- You have the SPECIAL attribute.
- The profile is within the scope of a group in which you have the group-SPECIAL attribute.
- You have the OPERATIONS attribute.
- The profile is within the scope of a group in which you have the group-OPERATIONS attribute.
- The userid qualifier of the file name is your user ID.
- You are the owner of the file.
- You have the AUDITOR or ROAUDIT attribute.
- The file profile is within the scope of a group in which you have the group-AUDITOR attribute.
- You have ALTER authority from the global access checking table (if this table contains an entry for the profile).

For discrete profiles only:

- You are on the profile's access list with ALTER authority. (If you have any other level of authority, you may not use the operand.)
- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is in the access list and has ALTER authority. (If any group that RACF checked has any other level of authority, you may not use the operand.)
- The universal access authority is ALTER.

Syntax

The complete syntax of the LFILE command is:

```
LFILE                {profile-name | * * *}
LF                   [ ALL ]
                     [ AUTHUSER ]
                     [ {GENERIC | NOGENERIC} ]
                     [ HISTORY ]
                     [ STATISTICS ]
```

Note: This command is an extension of the RLIST command as it applies to the FILE class. Other RLIST parameters, such as SESSION and DLFDATA are also accepted on the command, but are not listed here. If they are specified on this command, they will be processed as on RLIST, but they have no meaning for SFS.

Parameters

***profile-name* | * * ***

profile-name
specifies the name of the discrete or generic profile about which information is to be displayed. You may specify only one profile and the name must be in SFS format. For the format of these profile names, see "Profile Names for SFS Files and Directories" on page 342.

This operand or * * * is required.

*** * ***
specifies that you want to display information for all files for which you have proper authority.

ALL
specifies that you want all information for each file profile displayed.

The access list is not included unless you have sufficient authority to use the AUTHUSER operand, as described in "Authorization Required" on page 155. The list does not include the type of access attempts (as specified by the GLOBALAUDIT operand on the ALTDIR command) that are being logged on the SMF data file unless you have the AUDITOR or group-AUDITOR attribute.

AUTHUSER
specifies that you want to see the access list for each profile. The output shows the following:

- The user categories authorized to access the resource
- The security level required to access the resource
- The security label required to access the resource
- The standard access list. This includes the following:
  - All users and groups authorized to access the resource
  - The level of authority for each user and group
  - The number of times the user has accessed the resource[5]
- The conditional access list. This list consists of the same fields as in the standard access list, as well as the following fields:
  - The class of the resource via which each user and group in the list can access the target resource of the command. For example, if a user can access the target resource via terminal TERM01, then TERMINAL would be the class listed.
  - The entity name of the resource via which each user and group in the list can access the target resource of the command. In the example above, TERM01 would be listed.

You must have sufficient authorization to use the AUTHUSER operand, as described in "Authorization Required" on page 155.

GENERIC | NOGENERIC

GENERIC
specifies that you want RACF to display information for the generic profile that most closely matches an SFS file name. If you specify GENERIC, RACF ignores a discrete profile that protects the SFS file. If asterisks (* * *) are specified instead of the profile name, all generic file profiles will be listed.

NOGENERIC
specifies that you want RACF to display information for the discrete profile that protects an SFS file. If asterisks (* * *) are specified instead of the profile name, all generic file profiles will be listed.

[5] This detail is only meaningful when your installation is gathering resource statistics. For a generic profile, RACF replaces any statistics line with NOT APPLICABLE FOR GENERIC PROFILE.

If neither GENERIC nor NOGENERIC is specified, RACF lists information for the discrete file name that matches the file name you specify. If there is no matching discrete profile, RACF will list the generic profile that most closely matches the file name. If asterisks (* * *) is specified instead of the profile name, all discrete and generic profiles will be listed.

Assume the following profiles exist in the FILE class:

```
z/VM  SCRIPT   FP:LAURIE.DIR1
*   SCRIPT   FP:LAURIE.DIR1 (G)
*   *        FP:LAURIE.DIR1 (G)
ALL NOTEBOOK FP:LAURIE.DIR1
```

- If you enter

  ```
  LFILE ALL NOTEBOOK FP:LAURIE.DIR1 GENERIC
  ```

  RACF will list profile * * FP:LAURIE.DIR1 (best matching generic profile)
- If you enter

  ```
  LFILE ALL NOTEBOOK FP:LAURIE.DIR1
  ```

  RACF will list profile ALL NOTEBOOK FP:LAURIE.DIR1 (discrete profile found first)
- If you enter

  ```
  LFILE DEPT NOTEBOOK FP:LAURIE.DIR1 NOGENERIC
  ```

  RACF will not list any profiles, because no matching discrete profile exists (even though a matching generic does exist, * * FP:LAURIE.**)

HISTORY

specifies that you want to list the following data:

- Date each profile was defined to RACF
- Date each file was last referenced [6]
- Date of last RACROUTE REQUEST=AUTH for UPDATE authority. [6]

STATISTICS

specifies that you want to list the statistics for each profile. The list includes the number of times the profile was accessed by users with READ, UPDATE, CONTROL and ALTER authorities, as well as a separate total for each authority level. [6]

Examples

Example

Operation	User GARY wants to list the information for the profile protecting his file CHART SCRIPT in his DIR1 subdirectory.
Known	User GARY is RACF-defined and does not have the AUDITOR attribute.
Command	`LFILE CHART SCRIPT FP1:GARY.DIR1 ALL`
Defaults	None
Output	See Figure 3 on page 159.

[6] This detail is only meaningful when your installation is gathering resource statistics. For a generic profile, RACF replaces any statistics line with NOT APPLICABLE FOR GENERIC PROFILE.

```
LFILE CHART SCRIPT FP1:GARY.DIR1

     CLASS       NAME
     -----       ----
     FILE        CHART SCRIPT FP1:GARY.DIR1

     LEVEL  OWNER    UNIVERSAL ACCESS  YOUR ACCESS   WARNING
     -----  -------- ----------------  -----------   -------
      00    GARY          NONE             ALTER     NO

     INSTALLATION DATA
     -----------------
     NONE

     APPLICATION DATA
     -----------------
     NONE

     SECLEVEL
     --------
     NO SECLEVEL

     CATEGORIES
     ----------
     NO CATEGORIES

     SECLABEL
     ----------
     NO SECLABEL

     AUDITING
     --------
     FAILURES(READ)

     NOTIFY
     --------
     NO USER TO BE NOTIFIED

     CREATION DATE  LAST REFERENCE DATE  LAST CHANGE DATE
      (DAY) (YEAR)       (DAY) (YEAR)      (DAY) (YEAR)
     -------------  -------------------  ----------------
       071    95          076    95         076    95

     ALTER COUNT   CONTROL COUNT   UPDATE COUNT   READ COUNT
     -----------   -------------   ------------   ----------
       000000         000000         000000         000000

     USER      ACCESS   ACCESS COUNT
     ----      ------   ------ -----
     GARY      ALTER       000000

     NO ENTRIES IN CONDITIONAL ACCESS LIST
```

Figure 3. Example 1. Output for LFILE Command

LISTDSD (List Data Set Profile)

System environment

Data sets apply to z/OS systems only.

Purpose

Use the LISTDSD command to list information included in tape and DASD data set profiles. A data set profile consists of a RACF segment and, optionally, a DFP segment. The LISTDSD command provides you with the option of listing information contained in the entire data set profile (all segments), or listing the information contained only in a specific segment of the profile.

You can request the details for any number of profiles by giving the full name of each profile. You can also request the details for all profiles whose names are qualified by specific user IDs, group names, and/or character strings.

Note: RACF interprets dates with 2 digit years in the following way, YY represents the 2 digit year.

```
IF 70 < YY <= 99 THEN
   The date is interpreted as 19YY
IF 00 <= YY <= 70 THEN
   The date is interpreted as 20YY
```

Details RACF lists from the RACF segment of each profile. These consist of:

- The level
- The owner
- The type of access attempts (as specified by the AUDIT operand on the ADDSD or ALTDSD command) that are being logged on the SMF data set
- The universal access authority
- Your highest level of access authority
- The group under which the profile was created
- The data set type (tape, VSAM, non-VSAM, or MODEL)
- The retention period for a tape data set
- The type of access attempts (as specified by the GLOBALAUDIT operand on the ALTDSD command) that are being logged on the SMF data set (for auditors only)
- The volume serial number (volser) of the volume on which the data set resides.

  For both a single volume and multivolume VSAM data set, the volser represents the volume containing the catalog entry for the data set.

  For a non-VSAM data set, the volser represents the volume containing the data set itself. If it is a multivolume non-VSAM data set, a list of volsers is given. The list represents the volumes on which the protected data set resides. They are listed in the order in which they were defined.
- Unit information for the data set (if unit information had been specified in the UNIT operand on the ADDSD or ALTDSD command)
- Installation-defined data as specified on the DATA operand of the ADDSD or ALTDSD command.

  Note: If your installation is running with maximum security, this information will not be listed in your output. * SUPPRESSED * will appear under the installation data field. Only those with system SPECIAL will be allowed to list the field.

Additional details. You can request the following details by using the appropriate LISTDSD operands:

- Historical data, such as the date the data set was:

  - Defined to RACF
  - Last referenced
  - Last updated.

  (see the HISTORY operand)
- The number of times the data set was accessed by all users for each of the following access authorities:

  ALTER, CONTROL, UPDATE, READ, EXECUTE.

  (see the STATISTICS operand)

  Note: These details are not meaningful if resource statistics gathering is bypassed at your installation. For a generic profile, RACF replaces any statistics line with `NOT APPLICABLE FOR GENERIC PROFILE`.
- The standard access list, which displays:
  - All users and groups authorized to access the data set
  - The level of authority for each user and group
  - The number of times each user has accessed the data set.

  (see the AUTHUSER operand)
- The conditional access list, which displays the same fields as the standard access list as well as the following fields:
  - The class of the resource
  - The entity name of the resource.

  (see the AUTHUSER operand)
- The information listed below:
  - The user categories authorized to access the data set
  - The security level required to access the data set
  - The security label required to access the data set.

  (see the AUTHUSER operand)
- Details RACF lists from the DFP segment of the profile:
  - The user ID or group name of the data set resource owner.

  (see the DFP operand)

Related Commands

- To list a general resource profile, use the RLIST command as described in "RLIST (List General Resource Profile)" on page 248. (General resources include terminals, minidisks, and other resources defined in the class descriptor table.)
- To list a user profile, use the LISTUSER command as described in "LISTUSER (List User Profile)" on page 179.
- To list a group profile, use the LISTGRP command as described in "LISTGRP (List Group Profile)" on page 172.
- To list a SFS file profile, use the LFILE command as described in "LFILE (List SFS File Profile)" on page 154. (A file profile protects files in the z/VM shared file system.)
- To list a SFS directory profile, use the LDIRECT command as described in "LDIRECT (List SFS Directory Profile)" on page 148. (A directory profile protects directories in the z/VM shared file system.)

Authorization Required

This topic describes the authorization that is required.

Listing the RACF segment of a data set profile. To list the details of the RACF segment of a data set profile, you must have a sufficient level of authority for each profile listed as the result of your request. RACF makes the following checks for each profile until one of the conditions is met:

- You have the SPECIAL attribute.
- The profile is within the scope of a group in which you have the group-SPECIAL attribute.
- You have the OPERATIONS attribute.
- The profile is within the scope of a group in which you have the group-OPERATIONS attribute.
- The high-level qualifier of the profile name (or the qualifier supplied by a command installation exit) is your user ID.
- You are the owner of the profile.
- You are on the profile's access list with at least READ authority. (If your level of authority is NONE, the data set is not listed.)
- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is in the access list and has at least READ authority. (If the level of authority for any group that RACF checked is NONE, the data set is not listed.)
- The universal access authority is at least READ.
- You have at least READ access for the profile name from the GLOBAL ENTRY TABLE (if this table contains an entry for the profile).
- You have the AUDITOR or ROAUDIT attribute.
- The data set profile is within the scope of a group in which you have the group-AUDITOR attribute.

If you have the AUDITOR or ROAUDIT attribute, or the profile is within the scope of a group in which you have the group-AUDITOR attribute, the type of access attempts (as specified by the GLOBALAUDIT operand on the ALTDSD command) that are being logged on the SMF data set are also displayed.

When you specify the AUTHUSER operand to display the access list for a profile, RACF checks your level of authority for each profile until one of the following conditions is met:

- You have the SPECIAL attribute.
- You have the OPERATIONS attribute.
- The profile is within the scope of a group in which you have the group-SPECIAL attribute.
- The profile is within the scope of a group in which you have the group-OPERATIONS attribute.
- The high-level qualifier of the profile name (or the qualifier supplied by a command installation exit) is your user ID.
- You are the owner of the profile.
- You have ALTER access for the profile name from the GLOBAL ENTRY TABLE (if this table contains an entry for the profile).

For discrete profiles only:

- You are on the profile's access list with ALTER authority. (If you have any other level of authority, you cannot use the operand.)
- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is in the access list and has ALTER authority. (If any group that RACF checked has any other level of authority, you may not use the operand.)
- The universal access authority is ALTER.

For both discrete and generic profiles:

- You have the AUDITOR or ROAUDIT attribute.
- The data set profile is within the scope of a group in which you have the group-AUDITOR attribute.

Listing the DFP segment of a data set profile. To list information within the DFP segment of a data set profile, one of the following conditions must be true:

- You have the SPECIAL, AUDITOR, or ROAUDIT attribute.
- You have at least READ authority to the desired field within the DFP segment through field level access control.

Syntax

The complete syntax of the LISTDSD command is:

```
LISTDSD                 [ ALL ]
LD                      [ AUTHUSER ]
                        [ {DATASET(profile-name ...)
                          | ID(name ...)
                          | PREFIX(char ...)} ]
                        [ DFP ]
                        [ DSNS ]
                        [ GENERIC | NOGENERIC ]
                        [ HISTORY ]
                        [ NORACF ]
                        [ STATISTICS ]
                        [ VOLUME(volume-serial ...) ]
```

Parameters

ALL
specifies that you want all information for each data set displayed at your terminal.

The DFP segment must be requested explicitly.

The access list is not included unless you have sufficient authority to use the AUTHUSER operand (see "Authorization Required" on page 161). The list does not include the type of access attempts (as specified by the GLOBALAUDIT operand on the ALTDSD command) that are being logged on the SMF data set unless you have the AUDITOR, ROAUDIT, or group-AUDITOR attribute.

AUTHUSER
specifies that you want the following information included in the output:

- The user categories authorized to access the data set
- The security level required to access the data set
- The security label required to access the data set
- The standard access list. This contains the following:
  - All users and groups authorized to access the data set
  - The level of authority for each user and group
  - The number of times each user has accessed the data set[7]
- The conditional access list. This list consists of the same fields as in the standard access list, as well as the following fields:
  - The class of the resource via which each user and group can access the dataset. For example, if a user can access the dataset via terminal TERM01, then TERMINAL would be the class listed.
  - The entity name of the resource via which each user and group can access the dataset. In the example above, TERM01 would be listed.

You must have sufficient authorization to use the AUTHUSER operand (see "Authorization Required" on page 161).

[7] This detail is only meaningful when your installation is gathering resource statistics. This detail is not included in the output for generic profiles.

DATASET | ID | PREFIX

DATASET(*profile-name* ...)
specifies the names of one or more data sets whose profiles RACF is to list. If a specified name appears more than once in the RACF database, LISTDSD displays information about all the profiles with that name to which you have proper authority.

The data set name you specify must be enclosed in single quotation marks unless it is your own data set.

Note that, because RACF uses the RACF database and not the catalog when searching for data set profiles, you cannot use alias data set names.

ID(*name* ...)
specifies one or more user IDs or group names. All users and groups must be defined to RACF. Details are listed for all discrete and generic profiles that have the specified user IDs or group names as the high-level qualifier name (or as the qualifier supplied by a command installation exit).

If you do not specify DATASET, PREFIX, or ID, RACF uses your user ID as the default value for the ID operand.

PREFIX(*char* ...)
specifies one or more character strings. Details are listed for all profiles whose names begin with the specified character strings.

Note that comparison between the character strings and the profile names is not limited to the high-level qualifier. For example, if you specify PREFIX(A.B.C), RACF would display information for profiles such as A.B.C, A.B.CAD, and A.B.C.X.

DFP
specifies that, for a DFP-managed data set, you want to list the user ID or group name designated as the data set resource owner. (The data set resource owner, or RESOWNER, is distinguished from the OWNER, which represents the user or group that owns the data set profile.)

DSNS
specifies that you want to list the cataloged data sets protected by the profile specified by the DATASET, ID, or PREFIX operand.

Affected tape datasets will always be listed, regardless of what is specified for SETROPTS TAPE DSN, or whether the TAPEVOL class is active.

When data and index components of VSAM clusters are listed, they will be followed by (D) or (I) respectively.

The list of data sets may be inaccurate if one of the following is true:

- You are using naming convention processing, either through the naming convention table or an exit, to modify data set names so they are protected by different profiles.
- You are using the PREFIX operand of SETROPTS to provide a high-level qualifier for data sets that have only one level in their names.
- There are migrated items in the list and the migration facility is unavailable. If the facility is not available, migrated items are followed in the list by the message:

```
** Unable to verify this
** migrated item. (1)
```

The number in parentheses denotes diagnostic information.

Note:

1. If a migrated cluster name appears in the list, but it has an alternate index or path, information on its data or index names is unavailable without recalling the name. This message appears following the cluster name:

```
** Migrated cluster component information
** not available without recall.
```

2. If a migrated cluster name appears in the list and LISTDSD cannot obtain the index and data names due to a migration facility error, then this message appears following the cluster name:

```
** Migrated cluster component information
** not available.
```

3. If the catalog indicates that the item is migrated, but the migration facility has no record of it, then this message appears following the item name:

```
** Catalog and migration information
** are not consistent.
```

4. If the name of a non-migrated cluster appears in the list and RACF is unable to obtain the data and index names specifically through this item, this message appears following the cluster name:

```
** Cluster component information
** not available.
```

GENERIC | NOGENERIC

GENERIC
specifies that you want RACF to display information for the generic profile that most closely matches a data set. Note that if you specify GENERIC, RACF ignores a discrete profile that protects the data set, even if the data set is RACF-indicated.

NOGENERIC
specifies that you want RACF to display information for the discrete profile that protects a data set.

When specifying GENERIC or NOGENERIC, consider the following:

- If you specify either the ID or PREFIX operand but omit GENERIC and NOGENERIC, RACF lists information for **both discrete and generic** profiles.

  For example, if you enter the following command:

```
LISTDSD  ID(SMITH)
```

  RACF lists all data set profiles for user ID SMITH.

- If you specify the DATASET operand but omit GENERIC and NOGENERIC, RACF lists information for the **discrete** profile that matches the data set name you specify.

  For example, if you enter the following command:

```
LISTDSD  DATASET('XXX.YYY')
```

  RACF lists information for the discrete profile, XXX.YYY.

- If you want to list only the **generic** profile that protects a data set, you must specify the DATASET operand (with the data set name) and the GENERIC operand.

  For example, if you specify the following command:

```
LISTDSD  DATASET('XXX.YYY')  GENERIC
```

  RACF lists the fully qualified generic profile XXX.YYY if it exists, or the generic profile that most closely matches XXX.YYY.

- If generic profile command processing is inactive, RACF lists only discrete profiles; that is, RACF does not look for generic profiles.

HISTORY
specifies that you want to list the following data:

- The date each profile was defined to RACF
- The date each data set was last referenced
- The date of the last RACHECK for UPDATE authority.

NORACF
specifies that you want to suppress the listing of RACF segment information from the specified data set's profile. If you specify NORACF, you must include either the DSNS operand or the DFP operand, or both operands.

If you do not specify NORACF, RACF displays the information in the RACF segment of a dataset.

The information displayed as a result of using the NORACF operand is dependent on other operands used in the command. For example, if you use NORACF with DSNS or DFP also specified, only that information (DSNS or DFP) will be displayed.

STATISTICS
specifies that you want to list the statistics for each profile. The list includes the number of times the profile was accessed by users with READ, UPDATE, CONTROL, and ALTER authorities, as well as a separate total for each authority level. These details are meaningful only when your installation is gathering resource statistics. For generic profiles, RACF replaces any statistics line with `NOT APPLICABLE FOR GENERIC PROFILE`.

VOLUME(*volume-serial....*)
limits the profiles listed to those found on the specific volume or list of volumes identified by volume serial number. RACF does not list profiles with the same name found on other volumes. If you do not specify NOGENERIC, RACF will list any generic profiles as well.

Examples

Example 1

Operation	User DAF0 wants to list all information for his own data set profiles.
Known	User DAF0 is RACF-defined, and does not have the AUDITOR attribute.
Command	`LISTDSD ALL`
Defaults	ID(DAF0)
Output	See Figure 4 on page 168.

Example 2

Operation	User IA0 wants to list the users authorized to data set SYS1.PLIBASE.
Known	User IA0 has ALTER authority to SYS1.PLIBASE, and does not have the AUDITOR attribute.
Command	`LISTDSD DATASET('SYS1.PLIBASE') AUTHUSER`
Defaults	None
Output	See Figure 6 on page 170.

Example 3

Operation: User ADM1 wants to list a generic profile SALES.*.ABC.

Known: User ADM1 is the owner of the generic profile, and generic profile command processing is enabled. User ADM1 has the group-AUDITOR attribute in group SALES.

Command:
```
LISTDSD DATASET('SALES.*.ABC')
```

Defaults: None

Output: See Figure 7 on page 170.

Example 4

Operation: User JADAMS wants to display the discrete profile for the DFP-managed data set RESEARCH.TEST.DATA. JADAMS also wants to display the user or group who is the data set resource owner.

Known: User JADAMS is the owner of the profile protecting data set RESEARCH.TEST.DATA. User JADAMS has field level access of at least READ for the DFP segment.

Command:
```
LISTDSD DATASET('RESEARCH.TEST.DATA') DFP
```

Defaults: None

Output: See Figure 8 on page 171.

```
LISTDSD ALL
 INFORMATION FOR DATASET DAF0.DS2.DATA

 LEVEL  OWNER    UNIVERSAL ACCESS  WARNING  ERASE
 -----  -------- ----------------  -------  -----
  00    DAF0            READ         NO     NO

AUDITING
--------
SUCCESS(READ),FAILURES(ALTER)

NOTIFY
--------
NO USER TO BE NOTIFIED

YOUR ACCESS  CREATION GROUP  DATASET TYPE
-----------  --------------  ------------
NONE GIVEN        RESEARCH     NON-VSAM

VOLUMES ON WHICH DATASET RESIDES  UNIT
--------------------------------  ----
231406                            SYSDA

NO INSTALLATION DATA

              SECURITY LEVEL
-----------------------------------------
NO SECURITY LEVEL

CATEGORIES
----------
NOCATEGORIES

SECLABEL
----------
NO SECLABEL

CREATION DATE  LAST REFERENCE DATE  LAST CHANGE DATE
(DAY)  (YEAR)       (DAY)  (YEAR)     (DAY)  (YEAR)
-------------  ------------------  ----------------
 145     85          145     85        145     85

ALTER COUNT  CONTROL COUNT   UPDATE COUNT  READ COUNT
-----------  -------------   ------------  ----------
  00000          00010          00000        00010

  ID      ACCESS   ACCESS COUNT
-------   -------   ------------
IA0        READ       00010
ADM1       READ       00000
PROJECTA  UPDATE      00008

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

Figure 4. Example 1: Output for the LISTDSD Command Part 1 of 2

```
INFORMATION FOR DATASET DAF0.DS3.DATA

 LEVEL  OWNER    UNIVERSAL ACCESS  WARNING  ERASE
 -----  -------- ----------------  -------  -----
  00    DAF0            READ         NO     NO

AUDITING
--------
ALL(UPDATE)

NOTIFY
--------
NO USER TO BE NOTIFIED

YOUR ACCESS  CREATION GROUP  DATASET TYPE
-----------  --------------  ------------
NONE GIVEN      RESEARCH       NON-VSAM

VOLUMES ON WHICH DATASET RESIDES  UNIT
--------------------------------  ----
231406                            SYSDA

NO INSTALLATION DATA

              SECURITY LEVEL
-----------------------------------------
NO SECURITY LEVEL

CATEGORIES
----------
NOCATEGORIES

SECLABEL
----------
NO SECLABEL

CREATION DATE  LAST REFERENCE DATE  LAST CHANGE DATE
(DAY)  (YEAR)       (DAY)  (YEAR)     (DAY)  (YEAR)
-------------  ------------------  ----------------
 145     85          145     85        145     85

ALTER COUNT  CONTROL COUNT   UPDATE COUNT  READ COUNT
-----------  -------------   ------------  ----------
 00000           00000          00000        00010

  ID      ACCESS   ACCESS COUNT
-------   -------  ------------
NO ENTRIES IN STANDARD ACCESS LIST

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

Figure 5. Example 1: Output for the LISTDSD Command Part 2 of 2

```
LISTDSD  DATASET('SYS1.PL1BASE')  AUTHUSER
 INFORMATION FOR DATASET SYS1.PLIBASE

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

AUDITING
--------
SUCCESS(UPDATE)

NOTIFY
--------
NO USER TO BE NOTIFIED

YOUR ACCESS  CREATION GROUP   DATASET TYPE
-----------  --------------   ------------
   ALTER        SYS1            NON-VSAM

VOLUMES ON WHICH DATASET RESIDES  UNIT
--------------------------------  ----
231407                            SYSDA

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

              SECURITY LEVEL
-----------------------------------------
NO SECURITY LEVEL

CATEGORIES
----------
NOCATEGORIES

SECLABEL
----------
NO SECLABEL

  ID      ACCESS   ACCESS COUNT
-------   -------  ------------
ESH25     UPDATE      00009
PROJECTB   READ       00015
IA0        ALTER      00020

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

Figure 6. Example 2: Output for the LISTDSD Command

```
LISTDSD DATASET('SALES.*.ABC')
 INFORMATION FOR DATASET SALES.*.ABC (G)

 LEVEL  OWNER    UNIVERSAL ACCESS  WARNING  ERASE
 -----  -------- ----------------  -------  -----
  00    ADM1            READ         NO     NO

 AUDITING
 --------
 ALL(READ)

NOTIFY
--------
NO USER TO BE NOTIFIED

 YOUR ACCESS  CREATION GROUP  DATASET TYPE
 -----------  --------------  ------------
 NONE GIVEN      RESEARCH       NON-VSAM

 GLOBALAUDIT
 -----------
 NONE

 NO INSTALLATION DATA
```

Figure 7. Example 3: Output for the LISTDSD Command

```
LISTDSD DATASET('RESEARCH.TEST.DATA') DFP
 INFORMATION FOR DATASET RESEARCH.TEST.DATA

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

 AUDITING
 --------
 ALL(READ)

NOTIFY
--------
NO USER TO BE NOTIFIED

 YOUR ACCESS  CREATION GROUP  DATASET TYPE
 -----------  --------------  ------------
 NONE GIVEN      RESEARCH       NON-VSAM

 GLOBALAUDIT
 -----------
 NONE

 NO INSTALLATION DATA

DFP INFORMATION
---------------
RESOWNER= KSMITH
```

Figure 8. Example 4: Output for the LISTDSD Command

LISTGRP (List Group Profile)

System environment

This command applies to both z/OS and z/VM systems.

Purpose

Use the LISTGRP command to list details of specific RACF group profiles. A group profile consists of a RACF segment and, optionally, a DFP segment or an OVM segment, or both. The LISTGRP command provides you with the option of listing the information contained in the entire group profile (all segments), or listing the information contained only in a specific segment of the group profile.

Note: RACF interprets dates with 2 digit years in the following way, YY represents the 2 digit year.

```
IF 70 < YY <= 99 THEN
   The date is interpreted as 19YY
IF 00 <= YY <= 70 THEN
   The date is interpreted as 20YY
```

The details RACF lists from the RACF segment of each group profile are:

- The superior group of the group
- The owner of the group
- The terminal option of the group
- Any subgroups under the group
- Installation-defined data, as specified by the DATA operand of the ADDGROUP and ALTGROUP command
- The name of the data set model profile.

RACF lists the following information from the RACF segment of the group profile for each user connected to the group:

- The user ID
- The user's level of authority in the group
- The number of times the user has entered the system using this group as the current connect group
- The user's default universal access authority
- The user's connect attributes (group-related user attributes)
- Any REVOKEs or RESUMEs either in effect or pending, with the corresponding dates.

The details RACF lists from the DFP segment of the group profile are:

- The group's default data class
- The group's default management class
- The group's default storage class
- The data management data application for the group.

The details RACF lists from the OVM segment of the group profile are:

- The group's OpenExtensions group identifier.

Related Commands

- To list a user profile, use the LISTUSER command as described in “LISTUSER (List User Profile)” on page 179.

- To list a data set profile, use the LISTDSD command as described in "LISTDSD (List Data Set Profile)" on page 160.
- To list a general resource profile, use the RLIST command as described in "RLIST (List General Resource Profile)" on page 248. (General resources include terminals, minidisks, and other resources defined in the class descriptor table.)
- To list a file profile, use the LFILE command as described in "LFILE (List SFS File Profile)" on page 154. (A file profile protects files in the z/VM shared file system.)
- To list a directory profile, use the LDIRECT command as described in "LDIRECT (List SFS Directory Profile)" on page 148. (A directory profile protects directories in the z/VM shared file system.)

Authorization Required

Listing the RACF segment of a group profile. To list the details of the RACF segment of a group profile, one of the following conditions must be true:

- You have the SPECIAL attribute.
- You have the group-SPECIAL attribute in each group to be listed, or each group to be listed is within the scope of a group in which you have the group-SPECIAL attribute.
- You have the AUDITOR or ROAUDIT attribute.
- You have the group-AUDITOR attribute in each group to be listed, or each group to be listed is within the scope of a group in which you have the group-AUDITOR attribute.
- You are the owner of the group.
- You have JOIN or CONNECT authority in the group.

Listing the other segments of a group profile. To list information from segments other than the RACF segment of a group profile, one of the following conditions must be true:

- You have the SPECIAL, AUDITOR, or ROAUDIT attribute.
- You have at least READ authority to the desired field within the DFP or OVM segment via field level access control.

Syntax

The following operands used with the LISTGRP command apply to z/OS systems only:

- DFP

The complete syntax of the LISTGRP command is:

```
LISTGRP                                  [ {(group-name ...) | *} ]
LG                                       [ NORACF ]
                                         [ OVM ]

z/OS Specific Operands:
                                         [ DFP ]
```

Parameters

***group-name* | ***

group-name
specifies the name of one or more RACF-defined groups. If you specify more than one group name, you must enclose the names in parentheses.

*****
specifies that you want to list information contained in all RACF-defined group profiles to which you have the required authority.

If you specify a group name or *, it must be the first operand following LISTGRP.

If you enter LISTGRP and specify one or more group names (or *) without specifying an additional operand, RACF lists only the RACF segment information from the specified profiles.

If you enter only LISTGRP, RACF lists only the RACF segment information from your current connect group.

DFP

Note: *This operand applies to z/OS systems only.*

specifies that you want to list the information contained in the DFP segment of the group profile.

If you specify DFP (with or without NORACF), you must also specify a group name or *.

NORACF

specifies that you want to suppress the listing of base segment information from the group profile. If you specify NORACF, you must also specify DFP.

If you do not specify NORACF, RACF displays the information in the RACF segment of a group profile.

OVM

specifies that you want to list the information contained in the OVM segment of the group profile.

If you specify OVM (with or without NORACF), you must also specify a group name or *.

If the group profile contains an OVM segment but GID was not specified on a ADDGROUP or ALTGROUP command, the listing displays the field name followed by the word “NONE”.

Examples

Example 1	Operation	User IA0 wants to display the information contained in the RACF segment of the profile for group RESEARCH.
	Known	User IA0 has CONNECT authority to group RESEARCH.
	Command	`LISTGRP RESEARCH`
	Defaults	None
	Output	See Figure 9 on page 176.
Example 2	Operation	User ADM1 wants to display the information contained in the RACF segment of the profiles for all groups.
	Known	User ADM1 has the SPECIAL and AUDITOR attributes.
	Command	`LISTGRP *`
	Defaults	None
	Output	See Figure 10 on page 177.

LISTGRP Examples for z/OS:

Example 3

Operation: User ADM1 wants to display the information contained in the RACF segment and DFP segment of the profile for group DFPADMN.

Known: User ADM1 has the SPECIAL and AUDITOR attributes.

Group DFPADMN is defined to RACF, and DFPADMN's profile contains a DFP segment.

Command:
```
LISTGRP DFPADMN DFP
```

Defaults: None

Output: See Figure 11 on page 178.

Example 4

Operation: User ADM1 wants to display the information contained in only the DFP segment of the profile for group DFPADMN.

Known: User ADM1 has the SPECIAL and AUDITOR attributes.

Group DFPADMN is defined to RACF, and DFPADMN's profile contains a DFP segment.

Command:
```
LISTGRP DFPADMN DFP NORACF
```

Defaults: None

Output: See Figure 12 on page 178.

Example 5

Operation: User ADM1 requests the listing of the OVM segment for the group OVMG1.

Known: User ADM1 has the SPECIAL attribute.

Command:
```
LISTGRP OVMG1 OVM NORACF
```

Defaults: None

Output: See Figure 13 on page 178.

```
LISTGRP RESEARCH

INFORMATION FOR GROUP RESEARCH
    SUPERIOR GROUP=SYS1         OWNER=IBMUSER   CREATED=06.123
    NO INSTALLATION DATA
    NO MODEL DATA SET
    TERMUACC
    SUBGROUP(S)= PAYROLLB
    USER(S)=      ACCESS=      ACCESS COUNT=     UNIVERSAL ACCESS=
    IBMUSER         JOIN          000000              ALTER
       CONNECT   ATTRIBUTES=NONE
       REVOKE DATE=NONE                 RESUME DATE=NONE
    DAF0            JOIN          000002              READ
      CONNECT    ATTRIBUTES=NONE
      REVOKE DATE=NONE                 RESUME DATE=NONE
    IA0             CONNECT       000004              READ
      CONNECT    ATTRIBUTES=ADSP SPECIAL OPERATIONS
      REVOKE DATE=NONE                 RESUME DATE=NONE
    ESH25           USE           000000              READ
      CONNECT    ATTRIBUTES=NONE
      REVOKE DATE=NONE                 RESUME DATE=NONE
    PROJECTB        USE           000000              READ
      CONNECT    ATTRIBUTES=NONE
      REVOKE DATE=NONE                 RESUME DATE=NONE
    RV2             CREATE        000000              READ
      CONNECT    ATTRIBUTES=NONE
      REVOKE DATE=NONE                 RESUME DATE=NONE
    RV3             CREATE        000000              READ
      CONNECT    ATTRIBUTES=NONE
      REVOKE DATE=NONE                 RESUME DATE=NONE
    ADM1            JOIN          000000              READ
      CONNECT    ATTRIBUTES=OPERATIONS
      REVOKE DATE=NONE                 RESUME DATE=NONE
    AEH0            USE           000000              READ
      CONNECT    ATTRIBUTES=REVOKED
      REVOKE DATE=NONE                 RESUME DATE=NONE
```

Figure 9. Example 1: Output for LISTGRP RESEARCH

```
LISTGRP *

INFORMATION FOR GROUP PAYROLLB
    SUPERIOR GROUP=RESEARCH     OWNER=IBMUSER   CREATED=06.123
    NO INSTALLATION DATA
    NO MODEL DATA SET
    TERMUACC
    NO SUBGROUPS
    USER(S)=      ACCESS=      ACCESS COUNT=      UNIVERSAL ACCESS=
      IBMUSER       JOIN          000000              ALTER
         CONNECT ATTRIBUTES=NONE
         REVOKE DATE=NONE                   RESUME DATE=NONE
      DAF0          CREATE        000000              READ
         CONNECT ATTRIBUTES=NONE
         REVOKE DATE=NONE                   RESUME DATE=NONE
      IA0           CREATE        000000              READ
         CONNECT ATTRIBUTES=ADSP SPECIAL OPERATIONS
         REVOKE DATE=NONE                   RESUME DATE=NONE
      AEH0          CREATE        000000              READ
         CONNECT ATTRIBUTES=NONE
         REVOKE DATE=NONE                   RESUME DATE=NONE
INFORMATION FOR GROUP RESEARCH
    SUPERIOR GROUP=SYS1         OWNER=IBMUSER   CREATED=06.123
    NO INSTALLATION DATA
    NO MODEL DATA SET
    TERMUACC
    SUBGROUP(S)= PAYROLLB
    USER(S)=      ACCESS=      ACCESS COUNT=      UNIVERSAL ACCESS=
      IBMUSER       JOIN          000000              ALTER
         CONNECT ATTRIBUTES=NONE
         REVOKE DATE=NONE                   RESUME DATE=NONE
      DAF0          JOIN          000002              READ
         CONNECT ATTRIBUTES=NONE
         REVOKE DATE=NONE                   RESUME DATE=NONE
      IA0           CONNECT       000004              READ
         CONNECT ATTRIBUTES=ADSP SPECIAL OPERATIONS
         REVOKE DATE=NONE                   RESUME DATE=NONE
      ESH25         USE           000000              READ
         CONNECT ATTRIBUTES=NONE
         REVOKE DATE=NONE                   RESUME DATE=NONE
      PROJECTB      USE           000000              READ
         CONNECT ATTRIBUTES=NONE
         REVOKE DATE=NONE                   RESUME DATE=NONE
      RV2           CREATE        000002              READ
         CONNECT ATTRIBUTES=NONE
         REVOKE DATE=NONE                   RESUME DATE=NONE
      RV3           CREATE        000000              READ
         CONNECT ATTRIBUTES=NONE
         REVOKE DATE=NONE                   RESUME DATE=NONE
      ADM1          JOIN          000001              READ
         CONNECT ATTRIBUTES=OPERATIONS
         REVOKE DATE=NONE                   RESUME DATE=NONE
      AEH0          USE           000000              READ
         CONNECT ATTRIBUTES=NONE
         REVOKE DATE=NONE                   RESUME DATE=NONE
```

*Figure 10. Example 2: Output for LISTGRP **

```
LISTGRP DFPADMN DFP

INFORMATION FOR GROUP DFPADMN
    SUPERIOR GROUP=SYSADMN      OWNER=SYSADMN   CREATED=06.123
    NO INSTALLATION DATA
    NO MODEL DATA SET
    TERMUACC
    SUBGROUP(S)= DFPGRP1, DFPGRP2
    USER(S)=      ACCESS=      ACCESS COUNT=     UNIVERSAL ACCESS=
    IBMUSER          JOIN          000000              ALTER
       CONNECT   ATTRIBUTES=NONE
       REVOKE DATE=NONE                  RESUME DATE=NONE
    DSMITH           JOIN          000002              READ
      CONNECT    ATTRIBUTES=NONE
      REVOKE DATE=NONE                  RESUME DATE=NONE
    HOTROD           CONNECT       000004              READ
      CONNECT    ATTRIBUTES=ADSP SPECIAL OPERATIONS
      REVOKE DATE=NONE                  RESUME DATE=NONE
    ESHAW            USE           000000              READ
      CONNECT    ATTRIBUTES=NONE
      REVOKE DATE=NONE                  RESUME DATE=NONE
    PROJECTB         USE           000000              READ
      CONNECT    ATTRIBUTES=NONE
      REVOKE DATE=NONE                  RESUME DATE=NONE
    ADM1             JOIN          000000              READ
      CONNECT    ATTRIBUTES=OPERATIONS
      REVOKE DATE=NONE                  RESUME DATE=NONE
    AEHALL           USE           000000              READ
      CONNECT    ATTRIBUTES=REVOKED
      REVOKE DATE=NONE                  RESUME DATE=NONE
 DFP INFORMATION
    MGMTCLASS= DFP2MGMT
    STORCLASS= DFP2STOR
    DATACLAS= DFP2DATA
    DATAAPPL= DFP2APPL
```

Figure 11. Example 3: Output for LISTGRP DFPADMN DFP

```
LISTGRP DFPADMN DFP NORACF

INFORMATION FOR GROUP DFPADMN
 DFP INFORMATION
    MGMTCLASS= DFP2MGMT
    STORCLASS= DFP2STOR
    DATACLAS= DFP2DATA
    DATAAPPL= DFP2APPL
```

Figure 12. Example 4: Output for LISTGRP DFPADMN DFP NORACF

```
     LISTGRP OVMG1 OVM NORACF

    INFORMATION FOR GROUP OVMG1
      OVM INFORMATION
         GID= 0000003243
```

Figure 13. Example 5: Output for LISTGRP OVMG1 OVM NORACF

LISTUSER (List User Profile)

System environment

This command applies to both z/OS and z/VM systems.

Purpose

Use the LISTUSER command to list the details of specific RACF user profiles. A user profile consists of a RACF segment and, optionally, other segments such as TSO, OVM, or DFP. The LISTUSER command provides you with the option of listing the information contained in the entire user profile (all segments), or listing the information contained only in specific segments of the user profile.

Note: RACF interprets dates with 2 digit years in the following way, YY represents the 2 digit year.

```
IF 70 < YY <= 99 THEN
   The date is interpreted as 19YY
IF 00 <= YY <= 70 THEN
   The date is interpreted as 20YY
```

The details RACF lists from the RACF segment for each user profile are:

- The user ID
- The user's name or UNKNOWN, if the user's name was not specified on the ADDUSER command
- The owner of the user's profile
- The date the user was defined to RACF
- The default group
- The date the user's password was last updated
- The date the user's password phrase was last updated
- The change interval (in number of days)
- Whether the user password or password phrase is enveloped

  Note: This line is only displayed if enveloping is active, or if an envelope exists. If a user does not have a password or password phrase, the corresponding line will not be displayed.
- The user's attributes
- The date and time the user last entered the system
- The classes in which the user is authorized to define profiles
- The installation-defined data

  Note: If an installation is configured to be a B1 environment, this information will not be listed in your output. * SUPPRESSED * will appear under the installation data field. Only those with system SPECIAL will be allowed to list the field.
- The name of default data set model profile
- Any REVOKEs or RESUMEs either in effect or pending, with the corresponding dates
- The security label, the security level, and category.

In addition, RACF lists the following information from the RACF segment of the user profile for each group to which the user is connected:

- The group name
- The user's authority in the group
- The user ID of the person who connected the user to this group

- The date the user was connected to this group
- The number of times the user has entered the system with this group as the current connect group
- The default universal access authority
- The date and time the user last entered the system using this group as the current connect group
- The connect attributes (group-related user attributes).

The details RACF lists from the TSO segment of the user's profile are:

- The user's default account number when logging on from the TSO/E logon panel
- The destination ID for SYSOUT data sets
- The user's default HOLDCLASS
- The user's default JOBCLASS
- The user's default MSGCLASS
- The user's default SYSOUTCLASS
- The maximum region size
- The default region size
- The logon procedure name
- The unit name
- The optional user data
- The user's security label.
- MFA information: the level of detail is based on whether the MFA option is entered on input.

The details RACF lists from the DFP segment of the user's profile are:

- The user's default data class
- The user's default management class
- The user's default storage class
- The data management data application for the user.

The details RACF lists from the CICS segment of the user's profile are:

- The classes assigned to this operator to which BMS messages will be sent
- Whether the operator will be forced off when an XRFSOFF takeover occurs
- The operator identification
- The priority of the operator
- The time (in minutes) that the operator is allowed to be idle before being signed off.

The details RACF lists from the LANGUAGE segment of the user's profile are:

- The user's primary language, if one has been specified
- The user's secondary language, if one has been specified.

The details RACF lists from the OPERPARM segment of the user's profile are:

- The alternate console group (ALTGRP)
- The operator authority (AUTH)
- Whether the console receives messages which can be automated in a sysplex environment.
- The system name for commands from this console (CMDSYS)
- Whether, and what kind of, delete operator messages are received (DOM)
- The searching key (KEY)
- The message level information (LEVEL)
- Whether or not system command responses are logged (LOGCMDRESP)

- The message format (MFORM)
- Whether or not this console is assigned a migration ID (MIGID)
- Event information (MONITOR)
- The systems this console can receive undirected messages from (MSCOPE)
- Routing code information (ROUTCODE)
- Storage information (STORAGE)
- Whether or not this console receives undeliverable messages (UD).

The details RACF lists from the OVM segment of the user's profile are:

- The user identifier
- The initial directory pathname
- The program pathname
- The file system root name.

RACF lists the following output distribution information from the user's WORKATTR segment:

- The name of the user (WANAME)
- The building (WABLDG)
- The department (WADEPT)
- The room (WAROOM)
- Up to four additional lines of output distribution information (WAADDR1-4)
- An account number for APPC/MVS processing (WAACCNT).

Related Commands

- To list a group profile, use the LISTGRP command as describedon page “LISTGRP (List Group Profile)” on page 172.
- To list a data set profile, use the LISTDSD command as describedon page “LISTDSD (List Data Set Profile)” on page 160.
- To list a general resource profile, use the RLIST command as described on page “RLIST (List General Resource Profile)” on page 248. (General resources include terminals, minidisks, and other resources defined in the class descriptor table.)
- To list a file profile, use the LFILE command as described on page “LFILE (List SFS File Profile)” on page 154. (A file profile protects files in the z/VM shared file system.)
- To list a directory profile, use the LDIRECT command as described on page “LDIRECT (List SFS Directory Profile)” on page 148. (A directory profile protects directories in the z/VM shared file system.)

Authorization Required

Listing the RACF segment of a user profile

You can always list the details of the RACF segment of your own user profile. To list details of the RACF segment of another user's profile, one of the following conditions must be true:

- You are the owner of the user's profile.
- You have the SPECIAL attribute.
- The user's profile is within the scope of a group in which you have the group-SPECIAL attribute.
- You have the AUDITOR or ROAUDIT attribute.
- The user's profile is within the scope of a group in which you have the group-AUDITOR attribute.
- You have READ access to the IRR.LISTUSER resource in the FACILITY class and the user does not have the SPECIAL, AUDITOR, ROAUDIT, or OPERATIONS attribute.

- You have READ access to an appropriate resource (IRR.LU.OWNER.owner or IRR.LU.TREE.owner) in the FACILITY class, and both of the following conditions are also true:
  - The user does not have the SPECIAL, AUDITOR, ROAUDIT, or OPERATIONS attribute. (You can list a PROTECTED user.)
  - You are not excluded from listing the user by the IRR.LU.EXCLUDE.excludeduser resource in the FACILITY class.

  For more information about the IRR.LU profiles, see *z/VM: RACF Security Server Security Administrator's Guide*.

To list details of the RACF segment of all RACF-defined user profiles (by specifying the asterisk (*) operand), one of the following conditions must be true for each listed profile:

- You are the owner of the user's profile. RACF lists the RACF segment for all the user profiles that you own.
- You have the SPECIAL attribute. RACF lists the RACF segment for all user profiles.
- The user's profile is within the scope of a group in which you have the group-SPECIAL attribute. RACF lists the RACF segment for all the user profiles within the scope of your group.
- You have the AUDITOR or ROAUDIT attribute. RACF lists the RACF segment for all user profiles.
- The user's profile is within the scope of a group in which you have the group-AUDITOR attribute. RACF lists the RACF segment for all the user profiles within the scope of your group.
- You have READ access to the IRR.LISTUSER resource in the FACILITY class and the user does not have any of the SPECIAL, AUDITOR, ROAUDIT, or OPERATIONS attributes.

If you have the group-SPECIAL, AUDITOR, or group-AUDITOR attribute and your installation has assigned security levels and security categories to user profiles, you must have the following to be able to display the RACF segment of a user's profile:

- A security level equal to, or greater than, that in the user profile you are trying to display
- All security categories contained in the user profile you are trying to display contained in your own user profile.

If you have the AUDITOR or ROAUDIT attribute, or the profile is within the scope of a group in which you the group-AUDITOR attribute, RACF also lists the value of the UAUDIT/NOUAUDIT operand.

Listing the other segments of a user profile

To list information from segments other than the RACF segment for a user profile, including your own, one of the following conditions must be true:

- You have the SPECIAL, AUDITOR, or ROAUDIT attribute.
- You have at least READ authority to the desired field within the segment through field level access checking.

Syntax

The following operands used with the LISTUSER command apply to z/OS systems only:

- CICS
- DFP
- LANGUAGE
- OPERPARM
- TSO
- WORKATTR

The complete syntax of the LISTUSER command is:

LISTUSER LU	[(*userid* ...) | *] [MFA] [NORACF] [OVM]
z/OS Specific Operands:	
	[CICS] [DFP] [LANGUAGE] [OPERPARM] [TSO] [WORKATTR]

Parameters

***userid* | ***

userid
specifies the user ID of one or more RACF-defined users. If you specify more than one user ID, you must enclose the list of user IDs in parentheses.

*****
specifies that you want to list information contained in all RACF-defined user profiles to which you have the required authority.

If you specify a user ID or asterisk (*), it must be the first operand following LISTUSER.

If you enter LISTUSER and specify one or more user IDs (or *) without specifying an additional operand, RACF lists only the RACF segment information from the specified profiles.

If you enter only LISTUSER, RACF lists only the RACF segment information from your own user profile.

CICS

Note: *This operand applies to z/OS systems only.*

specifies that you want to list the information contained in the CICS segment of the user's profile.

If you specify CICS, you must also specify a user ID or *.

DFP

Note: *This operand applies to z/OS systems only.*

specifies that you want to list the information contained in the DFP segment of the user's profile.

If you specify DFP, you must also specify a user ID or *.

LANGUAGE

Note: *This operand applies to z/OS systems only.*

specifies that you want to list the information contained in the LANGUAGE segment of the user's profile.

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

If the code is displayed without a name, one of the following is true:

- RACF was not running under z/OS 4.1 or later releases
- The z/OS message service was not active
- The language was not active.

If the language code equals the language name, one of the following is true:

- There was no language name defined on your system

- The language name was defined to be the same as the language code.

If you specify LANGUAGE, you must also specify a user ID or *.

MFA
specifies that you want the IBM Multi-Factor Authentication (MFA) attributes listed. Messages will be displayed stating whether MFA is enabled for the user and (if enabled) whether password fallback is allowed.

If MFA is not specified and the user is an MFA user, the message "MULTIFACTOR AUTHENTICATION DATA EXISTS. USE THE MFA KEYWORD TO DISPLAY IT" will be displayed at the bottom of the LISTUSER output.

NORACF

specifies that you want to suppress the listing of RACF segment information from the user's profile.

If you specify NORACF, you must also specify one or more of these segments: WORKATTR, TSO, DFP, LANGUAGE, CICS, OPERPARM, or OVM.

If you do not specify NORACF, RACF displays the information in the RACF segment of a user profile.

The information displayed as a result of using the NORACF operand is dependent on other operands used in the command. For example, if you use NORACF with TSO or DFP also specified, only that information (TSO or DFP) will be displayed.

OPERPARM
Note: *This operand applies to z/OS systems only.*

specifies that you want to list the information contained in the OPERPARM segment of the user's profile.

If you specify this operand you must also specify a user ID or an asterisk (*).

If there is no information in a field in the user's profile for this segment, the field name will not be displayed. However, if no value was specified for STORAGE when the OPERPARM segment was added to the user profile, ST0RAGE=0 will appear in the listing.

OVM
specifies that you want to list the information contained in the OVM segment of the user's profile.

If you specify this operand, you must also specify a user ID or an asterisk (*).

If there is no HOME, PROGRAM, or FSROOT information, the field name is not displayed. However, the word “NONE” will appear in the listing if the UID was not specified, or if the UID was removed using the NOUID operand on the ALTUSER command.

TSO
Note: *This operand applies to z/OS systems only.*

specifies that you want to list the information contained in the TSO segment of the user's profile.

If you specify TSO, you must also specify a user ID or *.

If there is no information in the fields of the TSO segment, the field name is not displayed (with the exception of SIZE, MAXSIZE, and USERDATA).

WORKATTR
Note: *This operand applies to z/OS systems only.*

specifies that you want to list the information contained in the WORKATTR segment of the user's profile.

If you specify WORKATTR, you must also specify a user ID or an asterisk (*).

Examples

Example 1

Operation: User DAF0 wants to list her user attributes from the RACF segment of her user profile.

Known: DAF0 is a RACF-defined user with a password and password phrase. Both are enveloped.

Command:
```
LISTUSER
```

Defaults: DAF0 (userid)

Output: See Figure 14 on page 186.

Example 2

Operation: User DAF0 wants to list her user attributes from the RACF segment of her user profile.

Known: DAF0 is a RACF-defined password-only user. The password is enveloped.

Command:
```
LISTUSER
```

Defaults: DAF0 (userid)

Output: See Figure 15 on page 187.

Example 3

Operation: User DAF0 wants to list her user attributes from the RACF segment of her user profile.

Known: DAF0 is a RACF-defined phrase-only user. The password phrase is not enveloped.

Command:
```
LISTUSER
```

Defaults: DAF0 (userid)

Output: See Figure 16 on page 187.

Example 4

Operation: User DAF0 wants to list user attributes from the RACF segment of the SERVER1 user profile.

Known: SERVER1 is a RACF-defined user with no password or password phrase.

Command:
```
LISTUSER SERVER1
```

Defaults: DAF0 (userid)

Output: See Figure 17 on page 188.

Example 5

Operation: User ADM1 wants to list the user attributes from the RACF segment of profiles for users IBMUSER, CALTMANN, and DAF0.

Known: User ADM1 has the SPECIAL and AUDITOR attributes. User CALTMANN's password was recently reset and is expired, so his password change date appears as "00.000". Neither the password nor the password phrase is enveloped.

Command:
```
LISTUSER (IBMUSER CALTMANN DAF0)
```

Defaults: None

Output: See Figure 18 on page 188.

Example 6

Operation: User ADM1 wants to list the user attributes from the OVM segment of the profile for user CJWELLS.

Known: User ADM1 has the SPECIAL attribute.

User CJWELLS is defined to RACF and CJWELLS' profile contains an OVM segment.

Command: `LISTUSER CJWELLS OVM NORACF`

Defaults: None

Output: See Figure 20 on page 189.

Example 7

Operation: User ADM1 wants to list the user attributes from the OVM segment of the profile for user CBAKER.

Known: User ADM1 has the SPECIAL attribute.

User CBAKER is defined to RACF and CBAKER's profile contains an OVM segment, but there was no value specified for HOME, PROGRAM, or FSROOT in the OVM segment for this profile. Defaults were used.

Command: `LISTUSER CBAKER OVM NORACF`

Defaults: None

Output: See Figure 21 on page 189.

```
 LISTUSER

USER=DAF0     NAME=D.M.BROWN  OWNER=IBMUSER  CREATED=05.228
 DEFAULT-GROUP=RESEARCH  PASSDATE=05.228  PASS-INTERVAL= 30 PHRASEDATE=05.231
 ATTRIBUTES=PASSPHRASE
 PASSWORD ENVELOPED=YES
 PHRASE ENVELOPED=YES
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=05.228/13:31:11
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
 LOGON ALLOWED   (DAYS)          (TIME)
 ----------------------------------------
 ANYDAY                          ANYTIME
   GROUP=RESEARCH AUTH=JOIN    CONNECT-OWNER=IBMUSER   CONNECT-DATE=05.228
     CONNECTS=    01  UACC=READ    LAST-CONNECT=05.228/13:31:11
     CONNECT ATTRIBUTES=NONE
     REVOKE DATE=NONE   RESUME DATE=NONE
   GROUP=PAYROLLB AUTH=CREATE  CONNECT-OWNER=IBMUSER  CONNECT-DATE=05.228
     CONNECTS=   00  UACC=READ    LAST-CONNECT=UNKNOWN
     CONNECT ATTRIBUTES=NONE
     REVOKE DATE=NONE   RESUME DATE=NONE
 SECURITY-LEVEL=NONE SPECIFIED
 CATEGORY-AUTHORIZATION
  NONE SPECIFIED
```

Figure 14. Example 1: Output for LISTUSER

```
 LISTUSER

USER=DAF0     NAME=D.M.BROWN  OWNER=IBMUSER  CREATED=05.228
 DEFAULT-GROUP=RESEARCH  PASSDATE=05.228  PASS-INTERVAL= 30 PHRASEDATE=N/A
 ATTRIBUTES=NONE
 PASSWORD ENVELOPED=YES
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=05.228/13:31:11
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
 LOGON ALLOWED   (DAYS)          (TIME)
 -----------------------------------------
 ANYDAY                          ANYTIME
   GROUP=RESEARCH AUTH=JOIN    CONNECT-OWNER=IBMUSER   CONNECT-DATE=05.228
     CONNECTS=    01  UACC=READ    LAST-CONNECT=05.228/13:31:11
     CONNECT ATTRIBUTES=NONE
     REVOKE DATE=NONE   RESUME DATE=NONE
   GROUP=PAYROLLB AUTH=CREATE  CONNECT-OWNER=IBMUSER  CONNECT-DATE=05.228
     CONNECTS=   00  UACC=READ    LAST-CONNECT=UNKNOWN
     CONNECT ATTRIBUTES=NONE
     REVOKE DATE=NONE   RESUME DATE=NONE
 SECURITY-LEVEL=NONE SPECIFIED
 CATEGORY-AUTHORIZATION
  NONE SPECIFIED
```

Figure 15. Example 2: Output for LISTUSER

```
 LISTUSER

USER=DAF0     NAME=D.M.BROWN  OWNER=IBMUSER  CREATED=05.228
 DEFAULT-GROUP=RESEARCH  PASSDATE=N/A  PASS-INTERVAL= 30 PHRASEDATE=05.231
 ATTRIBUTES=NOPASSWORD PASSPHRASE
 PHRASE ENVELOPED=NO
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=05.228/13:31:11
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
 LOGON ALLOWED   (DAYS)          (TIME)
 -----------------------------------------
 ANYDAY                          ANYTIME
   GROUP=RESEARCH AUTH=JOIN    CONNECT-OWNER=IBMUSER   CONNECT-DATE=05.228
     CONNECTS=    01  UACC=READ    LAST-CONNECT=05.228/13:31:11
     CONNECT ATTRIBUTES=NONE
     REVOKE DATE=NONE   RESUME DATE=NONE
   GROUP=PAYROLLB AUTH=CREATE  CONNECT-OWNER=IBMUSER  CONNECT-DATE=05.228
     CONNECTS=   00  UACC=READ    LAST-CONNECT=UNKNOWN
     CONNECT ATTRIBUTES=NONE
     REVOKE DATE=NONE   RESUME DATE=NONE
 SECURITY-LEVEL=NONE SPECIFIED
 CATEGORY-AUTHORIZATION
  NONE SPECIFIED
```

Figure 16. Example 3: Output for LISTUSER

```
 LISTUSER SERVER1

USER=SERVER1   NAME=APP SERVER 1 OWNER=IBMUSER  CREATED=05.228
 DEFAULT-GROUP=SYS1  PASSDATE=N/A  PASS-INTERVAL= 30 PHRASEDATE=N/A
 ATTRIBUTES=PROTECTED
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=05.228/13:31:11
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
 LOGON ALLOWED   (DAYS)          (TIME)
 -----------------------------------------
 ANYDAY                          ANYTIME
   GROUP=SYS1 AUTH=USE   CONNECT-OWNER=IBMUSER   CONNECT-DATE=05.228
     CONNECTS=    01  UACC=READ    LAST-CONNECT=05.228/13:31:11
     CONNECT ATTRIBUTES=NONE
     REVOKE DATE=NONE   RESUME DATE=NONE
 SECURITY-LEVEL=NONE SPECIFIED
 CATEGORY-AUTHORIZATION
  NONE SPECIFIED
```

Figure 17. Example 4: Output for LISTUSER SERVER1

```
 LISTUSER (IBMUSER CALTMANN DAF0)

USER=IBMUSER  NAME=G. SMITH OWNER=IBMUSER  CREATED=05.163
 DEFAULT-GROUP=SYS1  PASSDATE=05.220  PASS-INTERVAL=N/A  PHRASEDATE=05.231
 ATTRIBUTES=SPECIAL OPERATIONS
 ATTRIBUTES=PASSPHRASE AUDITOR
 PASSWORD ENVELOPED=NO
 PHRASE ENVELOPED=NO
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=05.146/15:45:23
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
 LOGON ALLOWED   (DAYS)          (TIME)
 -----------------------------------------
 ANYDAY                          ANYTIME
  GROUP=SYS1      AUTH=JOIN    CONNECT-OWNER=IBMUSER  CONNECT-DATE=84.263
    CONNECTS=   456  UACC=READ    LAST-CONNECT=05.146/15:45:23
    CONNECT ATTRIBUTES=NONE
    REVOKE DATE=NONE   RESUME DATE=NONE
  GROUP=VSAMDSET  AUTH=JOIN    CONNECT-OWNER=IBMUSER  CONNECT-DATE=84.263
    CONNECTS=    00  UACC=NONE    LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=NONE
    REVOKE DATE=NONE   RESUME DATE=NONE
  GROUP=SYSCTLG   AUTH=JOIN    CONNECT-OWNER=IBMUSER  CONNECT-DATE=84.263
    CONNECTS=    00  UACC=READ    LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=NONE
    REVOKE DATE=NONE   RESUME DATE=NONE
 SECURITY-LEVEL=NONE SPECIFIED
 CATEGORY-AUTHORIZATION
  NONE SPECIFIED
 SECURITY-LABEL=NONE SPECIFIED
```

Figure 18. Example 5: Output for LISTUSER (IBMUSER CALTMANN DAF0) Part 1 of 2

```
USER=CALTMANN  NAME=C. ALTMANN  OWNER=IBMUSER   CREATED=05.144
 DEFAULT-GROUP=RESEARCH  PASSDATE=00.000 PASS-INTERVAL=254 PHRASEDATE=05.231
 ATTRIBUTES=SPECIAL
 ATTRIBUTES=PASSPHRASE AUDITOR
 PASSWORD ENVELOPED=NO
 PHRASE ENVELOPED=NO
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=05.146/16:16:14
 CLASS AUTHORIZATIONS=USER
 NO-INSTALLATION-DATA
 MODEL-NAME=ALLENA
 LOGON ALLOWED   (DAYS)          (TIME)
 ----------------------------------------
 ANYDAY                          ANYTIME
  GROUP=RESEARCH  AUTH=JOIN    CONNECT-OWNER=IBMUSER  CONNECT-DATE=05.144
    CONNECTS=    01  UACC=READ    LAST-CONNECT=05.146/16:16:14
    CONNECT ATTRIBUTES=OPERATIONS
    REVOKE DATE=NONE   RESUME DATE=NONE
  GROUP=VSAMDSET  AUTH=CREATE  CONNECT-OWNER=IBMUSER  CONNECT-DATE=05.144
    CONNECTS=    00  UACC=READ    LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=OPERATIONS
    REVOKE DATE=NONE   RESUME DATE=NONE
 SECURITY-LEVEL=NONE SPECIFIED
 CATEGORY-AUTHORIZATION
  NONE SPECIFIED
 SECURITY-LABEL=NONE SPECIFIED
USER=DAF0     NAME=D.M.BROWN  OWNER=IBMUSER  CREATED=05.144
 DEFAULT-GROUP=RESEARCH  PASSDATE=00.000 PASS-INTERVAL=254 PHRASEDATE=N/A
 ATTRIBUTES=NONE
 PASSWORD ENVELOPED=NO
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=05.146/15:11:31
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
 LOGON ALLOWED   (DAYS)          (TIME)
 ----------------------------------------
 ANYDAY                          ANYTIME
  GROUP=RESEARCH  AUTH=JOIN    CONNECT-OWNER=IBMUSER  CONNECT-DATE=05.144
    CONNECTS=    02  UACC=READ    LAST-CONNECT=05.146/15:11:31
    CONNECT ATTRIBUTES=NONE
    REVOKE DATE=NONE   RESUME DATE=NONE
 SECURITY-LEVEL=NONE SPECIFIED
 CATEGORY-AUTHORIZATION
  NONE SPECIFIED
 SECURITY-LABEL=NONE SPECIFIED
```

Figure 19. Example 5: Output for LISTUSER (IBMUSER CALTMANN DAF0) Part 2 of 2

```
 LISTUSER CJWELLS OVM NORACF
 USER=CJWELLS

 OVM INFORMATION
 ---------------
  UID= 0000000024
  HOME= /u/CJWELLS
  PROGRAM= /u/CJWELLS/bin/myshell
  FSROOT= /../VMBFS:SERVER8.CJWELLS/
```

Figure 20. Example 6: Output for LISTUSER CJWELLS OVM NORACF

```
 LISTUSER CBAKER OVM NORACF
 USER=CBAKER

 OVM INFORMATION
 ---------------
  UID= 0000000024
```

Figure 21. Example 7: Output for LISTUSER CBAKER OVM NORACF (Using Defaults)

PASSWORD or PHRASE (Specify User Password or Password Phrase)

System environment

This command applies to both z/OS and z/VM systems.

This command is usually called the PASSWORD command, though the PHRASE command is a supported alias.

Purpose

Use the PASSWORD command to:

- Change your current password or password phrase to a specified value
- Change a user's change interval (the number of days that a user's password and password phrase remain valid)
- Specify a password or password phrase that never expires
- Remove a user's password.

When a user's password is changed, RACF makes sure the new password is not the same as the current password. When SETR PASSWORD(HISTORY) is active, RACF also makes sure the new password is not already in the user's password history list. If the new password does not match one of these passwords, the current password is added to the user's password history list, and the new password is activated.

When a user's password phrase is changed, RACF makes sure the new password phrase is not the same as the current password phrase. When SETR PASSWORD(HISTORY) is active, RACF also makes sure the new password phrase is not already in the user's password phrase history list. If the new password phrase does not match one of these password phrases, the *new* password phrase is added to the user's password phrase history list, and the new password phrase is activated.

Related Commands

To change the installation change interval, see the PASSWORD operand on the SETROPTS command as described on page “SETROPTS (Set RACF Options)” on page 288.

Authorization Required

If you are a RACF-defined user and you are required to provide a RACF user password or password phrase when entering the system, you can change your own password, password phrase, or change interval.

To change another user's change interval, or to set a password and password phrase (if assigned) that never expire, you must have the SPECIAL attribute, or the user's profile must be within the scope of a group in which you have the group-SPECIAL attribute.

To remove a user's password, one of the following conditions must be true:

- You have the SPECIAL attribute
- The user's profile is within the scope of a group in which you have the group-SPECIAL attribute
- You are the owner of the user's profile.

Syntax

The complete syntax of the PASSWORD command is:

PASSWORD	[INTERVAL(*change-interval*) | NOINTERVAL]
PW	[PASSWORD(*current-password new-password*)]
PHRASE	[PHRASE('*current-password-phrase' 'new-password-phrase*')]
	[USER(*userid* ...)]

Parameters

INTERVAL | NOINTERVAL

INTERVAL(*change-interval*)
change-interval indicates the number of days during which a password or password phrase (if set) remain valid; the range is from 1 through 254 days.

The INTERVAL value you specify here cannot exceed the value, if any, that your installation has specified using the INTERVAL operand on the SETROPTS command. The initial system default after RACF initialization is 30 days.

The INTERVAL value you specify should not be less than the value (if any) that your installation specified using the MINCHANGE operand on the SETROPTS command. If this occurs, the user's password and password phrase (if set) cannot expire until your installation's minimum interval is reached and the user will not be allowed to change them prior to expiration.

If you specify INTERVAL on the PASSWORD command without a *change-interval* value, RACF uses the installation-specified maximum.

To specify INTERVAL with USER, you must have the SPECIAL attribute, or the user profile must be within the scope of a group in which you have the group-SPECIAL attribute. *Specifying INTERVAL with USER will not change or reset the user's password or password phrase.*

If you specify the interval incorrectly, RACF ignores this operand.

NOINTERVAL
specifies that neither a user's password nor password phrase (if set) will expire. To specify NOINTERVAL, you must have the SPECIAL attribute, or the user profile must be within the scope of a group in which you have the group-SPECIAL attribute.

Specifying NOINTERVAL without USER defines your own password or password phrase that never expires. *Specifying NOINTERVAL with USER will not change or reset the user's password or password phrase.*

The next time the user logs on, the user must select a new password or password phrase that will never expire.

You can use INTERVAL at any time to reinstate an expiration interval for a password or password phrase previously defined with NOINTERVAL.

PASSWORD(*current-password new-password*)
specifies your current password and the new one you want. From the RACF command session, if you enter only the PASSWORD operand, you are prompted so you can enter the current and new passwords in print inhibit mode.

The current and new passwords must have different values. When the installation allows mixed-case passwords, the old and new passwords cannot be the same characters with the case changed. If you specify your current password incorrectly, RACF notifies you and ignores the PASSWORD operand.

You can use the PASSWORD operand to change your own password at any time.

RACF ignores this operand when you specify the USER operand.

PHRASE('*current-password phrase' 'new-password phrase*')
Specifies your current password phrase and the new one you want. Each password phrase is a text string of up to 100 characters and must be enclosed in quotes. By default, a password phrase must be at least 14 characters long, but can be as short as 9 characters if the new-password-phrase exit (ICHPWX11) allows it.

Restriction: Because the password phrase value is a quoted string, The RACF command session does not support your entering it in *print inhibit* mode. Therefore, you should take care when entering your new password phrase to ensure it is not observed by others.

The current and new password phrases must have different values. If you specify your new current password phrase incorrectly, RACF notifies you and ignores the PHRASE operand.

The following rules apply to all password phrases. You cannot alter these syntax rules. You cannot add additional rules of your own unless your installation tailors the new-password-phrase exit (ICHPWX11). For programming details, see *z/VM: RACF Security Server System Programmer's Guide*.

Password Phrase Syntax Rules:

- Must not contain the user ID (as sequential uppercase or sequential lowercase characters)
- Must contain at least 2 alphabetic characters (A-Z, a-z)
- Must contain at least 2 non-alphabetic characters (numerics, punctuation, or special characters)
- Must not contain more than 2 consecutive characters that are identical
- Must be enclosed in single quotation marks, with single quotation marks within the password phrase doubled
- Must not contain forward slashes, nulls (X'00'), or leading or trailing blanks

If ICHPWX11 is present, it can reject the specified password phrase. Password phrases shorter than 14 characters will be rejected by RACF unless ICHPWX11 is present and allows the new value. If the specified password phrase is accepted, it is made the user's current password phrase and, when SETROPTS PASSWORD(HISTORY) is in effect, it is added to the user's password phrase history.

RACF ignores this operand when you specify the USER operand.

The PASSPHRASE attribute will appear in LISTUSER output for any user who has been assigned a password phrase.

USER(*userid* ...)
specifies one or more users whose password intervals are to be changed, or whose passwords are to be removed. If you specify USER without the INTERVAL operand, the user's password is removed.

When a user has no password, no password phrase, and is not enabled for MFA authentication, the user ID is a protected user. See *z/VM: RACF Security Server Security Administrator's Guide* for more information.

Examples

Example 1

Operation	User AEH0 wants to change his password from XY262 to YZ344 and increase his change interval to 60 days.
Known	User AEH0 is RACF-defined. The maximum installation change-interval is at least 60 days.
Command	`PASSWORD PASSWORD(XY262 YZ344) INTERVAL(60)`

Example 2

Operation	User ADM1 wants to remove the passwords for users CD0 and DAF0.
Known	User ADM1 has the group-SPECIAL attribute in group PAYROLL. Group PAYROLL is the owning group of users CD0 and DAF0. Users CD0 and DAF0 are RACF-defined.
Command	`PASSWORD USER(CD0 DAF0)`

Example 3

Operation: User ADM1 wants to set a password that never expires for user CD2.

Known: User ADM1 has the SPECIAL attribute. User CD2 is RACF-defined.

Command:
```
PASSWORD USER(CD2) NOINTERVAL
```

Example 4

Operation: User ADM1 wants to change his password phrase using the PHRASE alias of the PASSWORD command.

Known: User ADM1 is RACF-defined.

Command:
```
PHRASE PHRASE('This is my current password
phrase' 'This is my new password phrase.')
```

PERMDIR (Maintain SFS Directory Access Lists)

System environment

SFS directories apply to z/VM systems only.

Purpose

Use the PERMDIR command to maintain the lists of users and groups who are authorized to access a particular SFS directory or a group of SFS directories. RACF provides two types of access lists: standard and conditional.

The standard access list includes the user IDs and/or group names authorized to access the resource and the level of access granted to each.

The conditional access list includes user IDs and/or group names and levels of access, and it also includes for each, the name of the terminal by which the user must enter the system in order for RACF to allow access to the resource. The conditional access list is used for access checking only if the TERMINAL class is active.

You can maintain either the standard access list or the conditional access list with a single PERMDIR command. Changing both requires you to issue PERMDIR twice, with one exception. You can change individual names in one access list and copy the other access list from another profile on one PERMDIR command.

Using PERMDIR, you can make the following changes to either a standard access list or conditional access list for an SFS directory:

- Give specific RACF-defined users or groups authority to access a discrete or generic directory profile
- Remove authority to access a discrete or generic directory profile from specific users or groups
- Change the level of access authority to a discrete or generic directory profile for specific users or groups
- Copy the list of authorized users from one discrete or generic directory profile to another profile of either type and modify the new list as you require
- Delete an existing access list.

To have changes take effect after altering a generic profile, one of the following steps is required:

- The security administrator issues the SETROPTS command:

```
SETROPTS GENERIC(DIRECTRY) REFRESH
```

- The user of the resource logs off and logs on again

Related Commands

- To protect an SFS directory with a discrete or generic profile, use the ADDDIR command as described in “ADDDIR (Add SFS Directory Profile)” on page 16.
- To change an SFS directory profile, use the ALTDIR command as described in “ALTDIR (Alter SFS Directory Profile)” on page 66.
- To delete an SFS directory profile, use the DELDIR command as described in “DELDIR (Delete SFS Directory Profile)” on page 134.
- To list the information in the SFS directory profiles, use the LDIRECT command as described in “LDIRECT (List SFS Directory Profile)” on page 148.
- To obtain a list of SFS directory profiles, use the SRDIR command as described in “SRDIR (Obtain a List of SFS Directory Profiles)” on page 324.

Authorization Required

To perform any of the PERMDIR functions, you must have sufficient authority over the directory. RACF makes the following checks until one of the conditions is met:

- You have the SPECIAL attribute.
- The profile is within the scope of a group in which you have the group-SPECIAL attribute.
- You are the owner of the profile.
- Your user ID matches the user ID qualifier in the directory name.

For discrete profiles only:

- You are on the standard access list for the directory profile and you have ALTER authority.
- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is on the standard access list and has ALTER authority.
- The universal access authority is ALTER.

When you are copying a list of authorized users from one directory profile to another, you must have sufficient authority to both of the profiles as described in the preceding list.

Syntax

The complete syntax of the command is:

```
PERMDIR             profile-name-1
PDIR                [ ACCESS(access-authority) |  DELETE ]
                    [ FCLASS(profile-name-2-class) ]
                    [ FGENERIC ]
                    [ FROM(profile-name-2) ]
                    [ ID(name ...) ]
                    [ RESET [( ALL | STANDARD | WHEN )] ]
                    [ WHEN(TERMINAL(terminal-id ...) ) ]
```

Note: This command is an extension of the PERMIT command as it applies to the DIRECTRY class. Other PERMIT parameters, such as WHEN(PROGRAM) are also accepted on the command, but are not listed here. If they are specified on this command, they will be ignored.

Parameters

profile-name-1
specifies the name of an existing discrete or generic profile whose access list you want to modify. You can specify only one profile. For the format of these profile names, see "Profile Names for SFS Files and Directories" on page 342.

This operand is required and must be the first operand following PERMDIR.

ACCESS | DELETE

ACCESS(*access-authority*)
specifies the access authority you want to associate with the names that you identify on the ID operand. RACF sets the access authority in the standard access list.

If you specify WHEN, RACF sets the access authority in the conditional access list.

The valid access authorities are NONE, READ, UPDATE, CONTROL, and ALTER. (See "Access Authority for SFS Files and Directories on z/VM" on page 12 or if you need more information, see *z/VM: RACF Security Server Security Administrator's Guide*.)

If you specify ACCESS and omit *access-authority*, the default value is ACCESS(READ).

If you specify the ID operand and omit both ACCESS and DELETE, the default value is ACCESS(READ).

If you specify both ACCESS and DELETE, RACF uses the last operand you specify.

DELETE
specifies that you are removing the names you identify on the ID operand from the standard access list for the directory. RACF deletes the names from the standard access list.

If you specify WHEN, RACF deletes the names from the conditional access list.

If you specify the ID operand and omit both ACCESS and DELETE, the default value is ACCESS(READ).

If you specify both ACCESS and DELETE, RACF uses the last operand you specify.

FCLASS(*profile-name-2-class*)
specifies the name of the class to which *profile-name-2* belongs. The valid class names are DIRECTRY, FILE, DATASET, or those classes defined in the class descriptor table (CDT). For a list of general resource classes supplied by IBM, see Appendix B, "IBM-Supplied Resource Classes that Apply to z/VM Systems," on page 349.

If you specify FROM and omit FCLASS, RACF assumes that the class for *profile-name-2* is DIRECTRY. This operand is valid only when you also specify the FROM operand; otherwise, RACF ignores it.

FGENERIC
specifies that RACF is to treat *profile-name-2* as a generic name, even if it does not contain any generic characters. This operand is only needed if *profile-name-2* is a DATASET profile.

FROM(*profile-name-2*)
specifies the name of the existing discrete or generic profile that contains the access lists RACF is to copy as the access lists for *profile-name-1*. If you specify FROM and omit FCLASS, RACF assumes that *profile-name-2* is the name of a profile in the DIRECTRY class. If FCLASS is not specified, or FCLASS(DIRECTRY) is specified, *profile-name-2* must be the name of an existing profile in the DIRECTRY class. If FCLASS(FILE) is specified, *profile-name-2* must be the name of an existing profile in the FILE class. For the format of these profile names, see "Profile Names for SFS Files and Directories" on page 342.

If *profile-name-2* contains a standard access list, RACF copies it to the profile you are changing. If *profile-name-2* contains a conditional access list, RACF copies it to the profile you are changing.

RACF modifies the access list for *profile-name-1* as follows:

- Authorizations for *profile-name-2* are added to the access list for *profile-name-1*
- If a group or user appears in both lists, RACF uses the authorization granted in *profile-name-1*
- If you specify a group or user on the ID operand and that group or user also appears in the *profile-name-2* access list, RACF uses the authorization granted on the ID operand.

To specify FROM, you must have sufficient authority to both *profile-name-1* and *profile-name-2*, as described in "Authorization Required" on page 195.

ID(*name ...*)
specifies the user IDs and group names of RACF-defined users or groups whose authority to access the directory you are giving, removing, or changing. If you omit this operand, RACF ignores the ACCESS and DELETE operands.

RESET (ALL | STANDARD | WHEN)

RESET | RESET(ALL)
specifies that RACF is to delete from the profile both the entire current standard access list and the entire current conditional access list.

RACF deletes both access lists before it processes any operands (ID and ACCESS or FROM) that create new entries in an access list. If you delete both access lists and specify FROM when *profile-name-2* contains two access lists, the PERMDIR command copies both access lists to

profile-name-1. In any other situation, you cannot, on one PERMDIR command, add entries to both access lists.

If you specify RESET or RESET(ALL), add entries, and omit WHEN, RACF deletes both access lists, then adds entries to the standard access list.

If you specify RESET or RESET(ALL), add entries, and specify WHEN, RACF deletes both access lists, then adds entries to the conditional access list.

For profiles that include two access lists, use RESET and RESET(ALL) carefully. Unless you are copying both lists from another profile, it is a good practice to use RESET(STANDARD) to maintain the standard access list and RESET(WHEN) to maintain the conditional access list.

RESET(STANDARD)
specifies that RACF is to delete the entire current standard access list from the profile.

If you specify RESET(STANDARD) with ID and ACCESS or with FROM, RACF deletes the current standard access list from the profile before it adds the new names.

If you specify RESET(STANDARD) with ID and DELETE, RACF ignores RESET(STANDARD) and deletes only the names that you specify.

If you specify RESET(STANDARD) without ID and ACCESS, or without FROM, the resulting standard access list will be empty. An empty standard access list means that you must be the owner or have the SPECIAL attribute, or the profile must be within the scope of a group in which you have the group-SPECIAL attribute, in order to update the access list again.

RESET(WHEN)
RESET(WHEN) specifies that RACF is to delete the entire current conditional access list from the profile.

If you specify RESET(WHEN) with ID and ACCESS or with FROM, RACF deletes the current conditional access list from the profile before it adds the new names.

If you specify RESET(WHEN) with ID, DELETE, and WHEN, RACF ignores RESET(WHEN) and deletes only the names that you specify.

If you specify RESET(WHEN) without ID and ACCESS, or without FROM, the resulting conditional access list will be empty.

WHEN(TERMINAL(*terminal-id ...*))
specifies that the indicated users or groups have the specific access authority when logged on to the named terminal.

Examples

Example

Operation: User LAURIE wants to let user MARK look at her RACDEV directory.

Known: LAURIE and MARK are RACF-defined and LAURIE's file pool ID is FP1.

Command:
```
PERMDIR FP1:LAURIE.RACDEV ID(MARK)
```

Defaults: ACCESS(READ)

PERMFILE (Maintain SFS File Access Lists)

System environment

SFS directories apply to z/VM systems only.

Purpose

Use the PERMFILE command to maintain the lists of users and groups who are authorized to access a particular SFS file or a group of SFS files. RACF provides two types of access lists: standard and conditional.

The **standard access list** includes the user IDs and/or group names authorized to access the resource and the level of access granted to each.

The **conditional access list** includes user IDs and/or group names and levels of access, and it also includes for each, the name of the terminal by which the user must enter the system in order for RACF to allow access to the resource. The conditional access list is used for access checking only if the TERMINAL class is active.

You can maintain either the standard access list or the conditional access list with a single PERMFILE command. Changing both requires you to issue PERMFILE twice, with one exception. You can change individual names in one access list and copy the other access list from another profile on one PERMFILE command.

Using PERMFILE, you can make the following changes to either a standard access list or a conditional access list for an SFS file:

- Give authority to access a discrete or generic file profile to specific RACF-defined users or groups
- Remove authority to access a discrete or generic file profile from specific users or groups
- Change the level of access authority to a discrete or generic file profile for specific users or groups
- Copy the list of authorized users from one discrete or generic file profile to another profile of either type and modify the new list as you require
- Delete an existing access list.

To have changes take effect after altering a generic profile, one of the following steps is required:

- The security administrator issues the SETROPTS command:

```
SETROPTS GENERIC(FILE) REFRESH
```

- The user of the resource logs off and logs on again

Related Commands

- To protect an SFS file with a discrete or generic profile, use the ADDFILE command as described in “ADDFILE (Add SFS File Profile)” on page 22.
- To change an SFS file, use the ALTFILE command as described in “ALTFILE (Alter SFS File Profile)” on page 81.
- To delete an SFS file profile, use the DELFILE command as described in “DELFILE (Delete SFS File Profile)” on page 139.
- To list the information in the SFS file profile(s), use the LFILE command as described in “LFILE (List SFS File Profile)” on page 154.
- To obtain a list of SFS file profiles, use the SRFILE command as described in “SRFILE (Obtain a List of SFS File Profiles)” on page 329.

Authorization Required

To perform any of the PERMFILE functions, you must have sufficient authority over the file. RACF makes the following checks until one of the conditions is met:

- You have the SPECIAL attribute.
- The profile is within the scope of a group in which you have the group-SPECIAL attribute.
- You are the owner of the profile.
- Your user ID matches the user ID qualifier in the file name.

For discrete profiles only:

- You are on the standard access list for the file profile and you have ALTER authority.
- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is on the standard access list and has ALTER authority.
- The universal access authority is ALTER.

When you are copying a list of authorized users from one file profile to another, you must have sufficient authority, as described in the preceding list, to both of the profiles.

Syntax

The complete syntax of the command is:

```
PERMFILE          profile-name-1
PF                [ ACCESS(access-authority) | DELETE ]
                  [ FCLASS(profile-name-2-class) ]
                  [ FGENERIC ]
                  [ FROM(profile-name-2) ]
                  [ ID(name ...) ]
                  [ RESET [( ALL | STANDARD | WHEN )] ]
                  [ WHEN(TERMINAL(terminal-id ...) ) ]
```

Note: This command is an extension of the PERMIT command as it applies to the FILE class. Other PERMIT parameters, such as WHEN(PROGRAM) are also accepted on the command, but are not listed here. If they are specified on this command, they will be ignored.

Parameters

profile-name-1
specifies the name of an existing discrete or generic profile whose access list you want to modify. You can specify only one profile. For the format of these profile names, see "Profile Names for SFS Files and Directories" on page 342.

This operand is required and must be the first operand following PERMFILE.

ACCESS | DELETE

ACCESS(*access-authority*)
specifies the access authority you want to associate with the names that you identify on the ID operand. RACF sets the access authority in the standard access list.

If you specify WHEN, RACF sets the access authority in the conditional access list.

The valid access authorities are NONE, READ, UPDATE, CONTROL, and ALTER. See "Access Authority for SFS Files and Directories on z/VM" on page 12 if you need more information, or see *z/VM: RACF Security Server Security Administrator's Guide*.)

If you specify ACCESS and omit *access-authority*, the default value is ACCESS(READ).

If you specify the ID operand and omit both ACCESS and DELETE, the default value is ACCESS(READ).

If you specify both ACCESS and DELETE, RACF uses the last operand you specify.

DELETE
specifies that you are removing the names you identify on the ID operand from the standard access list for the file. RACF deletes the names from the standard access list.

If you specify WHEN, RACF deletes the names from the conditional access list.

If you specify the ID operand and omit both ACCESS and DELETE, the default value is ACCESS(READ).

If you specify both ACCESS and DELETE, RACF uses the last operand you specify.

FCLASS(*profile-name-2-class*)
specifies the name of the class to which *profile-name-2* belongs. The valid class names are DIRECTRY, FILE, DATASET, or those classes defined in the class descriptor table (CDT). For a list of general resource classes supplied by IBM, see Appendix B, "IBM-Supplied Resource Classes that Apply to z/VM Systems," on page 349.

If you specify FROM and omit FCLASS, RACF assumes that the class for *profile-name-2* is FILE. This operand is valid only when you also specify the FROM operand; otherwise, RACF ignores it.

FGENERIC
specifies that RACF is to treat *profile-name-2* as a generic name, even if it does not contain any generic characters. This operand is only needed if *profile-name-2* is a DATASET profile.

FROM(*profile-name-2*)
specifies the name of the existing discrete or generic profile that contains the access lists RACF is to copy as the access lists for *profile-name-1*. If you specify FROM and omit FCLASS, RACF assumes that *profile-name-2* is the name of a profile in the FILE class. If FCLASS is not specified, or FCLASS(FILE) is specified, *profile-name-2* must be the name of an existing profile in the FILE class. If FCLASS(DIRECTRY) is specified, *profile-name-2* must be the name of an existing profile in the DIRECTRY class. For the format of these profile names, see "Profile Names for SFS Files and Directories" on page 342.

If *profile-name-2* contains a standard access list, RACF copies it to the profile you are changing. If *profile-name-2* contains a conditional access list, RACF copies it to the profile you are changing.

RACF modifies the access list for *profile-name-1* as follows:

- Authorizations for *profile-name-2* are added to the access list for *profile-name-1*.
- If a group or user appears in both lists, RACF uses the authorization granted in *profile-name-1*.
- If you specify a group or user on the ID operand and that group or user also appears in the *profile-name-2* access list, RACF uses the authorization granted on the ID operand.

To specify FROM, you must have sufficient authority to both *profile-name-1* and *profile-name-2*, as described in "Authorization Required" on page 199.

ID(*name ...*)
specifies the user IDs and group names of RACF-defined users or groups whose authority to access the file you are giving, removing, or changing. If you omit this operand, RACF ignores the ACCESS and DELETE operands.

RESET (ALL | STANDARD | WHEN)

RESET | RESET(ALL)
specifies that RACF is to delete from the profile both the entire current standard access list and the entire current conditional access list.

RACF deletes both access lists before it processes any operands (ID and ACCESS or FROM) that create new entries in an access list. If you delete both access lists and specify FROM when *profile-name-2* contains two access lists, the PERMFILE command copies both access lists to

profile-name-1. In any other situation, you cannot, on one PERMFILE command, add entries to both access lists.

If you specify RESET or RESET(ALL), add entries, and omit WHEN, RACF deletes both access lists, then adds entries to the standard access list.

If you specify RESET or RESET(ALL), add entries, and specify WHEN, RACF deletes both access lists, then adds entries to the conditional access list.

For profiles that include two access lists, use RESET and RESET(ALL) carefully. Unless you are copying both lists from another profile, it is a good practice to use RESET(STANDARD) to maintain the standard access list and RESET(WHEN) to maintain the conditional access list.

RESET(STANDARD)
specifies that RACF is to delete the entire current standard access list from the profile.

If you specify RESET(STANDARD) with ID and ACCESS or with FROM, RACF deletes the current standard access list from the profile before it adds the new names.

If you specify RESET(STANDARD) with ID and DELETE, RACF ignores RESET(STANDARD) and deletes only the names that you specify.

If you specify RESET(STANDARD) without ID and ACCESS, or without FROM, the resulting standard access list will be empty. An empty standard access list means that you must be the owner or have the SPECIAL attribute, or the profile must be within the scope of a group in which you have the group-SPECIAL attribute, in order to update the access list again.

RESET(WHEN)
RESET(WHEN) specifies that RACF is to delete the entire current conditional access list from the profile.

If you specify RESET(WHEN) with ID and ACCESS or with FROM, RACF deletes the current conditional access list from the profile before it adds the new names.

If you specify RESET(WHEN) with ID, DELETE, and WHEN, RACF ignores RESET(WHEN) and deletes only the names that you specify.

If you specify RESET(WHEN) without ID and ACCESS, or without FROM, the resulting conditional access list will be empty.

WHEN(TERMINAL(*terminal-id ...*))
specifies that the indicated users or groups have the specific access authority when logged on to the named terminal.

Examples

Example

Operation: User SUE wants user EILEEN to be able to update the REPORT SCRIPT in her PAYROLL directory.

Known: SUE and EILEEN are RACF-defined and SUE's file pool ID is FP2.

Command:
```
PERMFILE REPORT SCRIPT FP2:SUE.PAYROLL
ACC(UPDATE) ID(EILEEN)
```

Defaults: None

PERMIT (Maintain Resource Access Lists)

System environment

Purpose

Use the PERMIT command to maintain the lists of users and groups authorized to access a particular resource. RACF provides two types of access lists: standard and conditional.

Standard Access List
The standard access list includes the user IDs and/or group names authorized to access the resource and the level of access granted to each.

Conditional Access List
The conditional access list includes user IDs and/or group names and levels of access, and also includes one of the following conditions for each. The condition is needed for RACF to allow access to the resource:

1. The name of the program the user must be executing
2. The name of the terminal by which the user entered the system
3. The name of the JES input device through which the user entered the system
4. The name of the system console from which the request was originated
5. The name of the APPC partner LU (logical unit) from which the transaction program originated.

If one of the criteria above is met, RACF uses both the standard and conditional access lists when it checks a user's authority to access a resource; otherwise RACF uses only the standard access list. For more information on conditional access lists or program control, refer to “Attribute and Authority Summary” on page 11.

You can maintain either the standard access list or the conditional access list with a single PERMIT command. Changing both requires you to issue PERMIT twice, with one exception. You can change individual names in one access list and copy the other access list from another profile on one PERMIT command.

Using PERMIT, you can make the following changes to either a standard access list or a conditional access list:

- Give authority to access a discrete or generic resource profile to specific RACF-defined users or groups
- Remove authority to access a discrete or generic resource profile from specific users or groups
- Change the level of access authority to a discrete or generic resource profile for specific users or groups
- Copy the list of authorized users from one discrete or generic resource profile to another profile of either type and modify the new list as you require
- Delete an existing access list.

For more information, refer to *z/VM: RACF Security Server Security Administrator's Guide*.

Related Commands

- To specify the default access rights (UACC) for a general resource (such as a z/VM minidisk or a terminal), use the RDEFINE command as described in “RDEFINE (Define General Resource Profile)” on page 225 (when creating a new profile), or the RALTER command as described in “RALTER (Alter General Resource Profile)” on page 213 (to change an existing profile).

Authorization Required

To perform any of the PERMIT functions, you must have sufficient authority over the resource. RACF makes the following checks until one of the conditions is met:

- You have the SPECIAL attribute
- The profile is within the scope of a group in which you have the group-SPECIAL attribute
- You are the owner of the resource
- If the resource belongs to the FILE or DIRECTRY class, the userid qualifier of the profile name matches your user ID, indicating that you are the owner of the referenced file or directory.

For discrete profiles in classes other than VMMDISK:

- You are on the standard access list for the resource and you have ALTER authority
- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is on the standard access list and has ALTER authority
- The universal access authority is ALTER.

When you are copying a list of authorized users from one resource profile to another, you must have sufficient authority, as described in the preceding list, to both of the resources.

Syntax

The complete syntax of the command is:

```
PERMIT          profile-name-1
PE              [ ACCESS(access-authority) | DELETE ]
                [ CLASS(profile-name-1-class) ]
                [ FCLASS(profile-name-2-class) ]
                [ FROM(profile-name-2) ]
                [ GENERIC ]
                [ ID( {name ... |*}) ]
                [ RESET [ (ALL | STANDARD | WHEN) ]
                [ WHEN( [TERMINAL(terminal-id ...)]
```

Parameters

profile-name-1
specifies the name of an existing discrete or generic profile whose access list you want to modify. You may specify only one profile.

This operand is required and must be the first operand following PERMIT.

If the name specified is a tape volume serial number that is a member of a tape volume set, the authorization assigned by this command will apply to all the volumes in the volume set.

If the profile does not belong to the DATASET class, you must also specify CLASS.

ACCESS | DELETE

ACCESS(*access-authority*)
specifies the access authority you want to associate with the names that you identify on the ID operand. RACF sets the access authority in the standard access list.

If you specify WHEN, RACF sets the access authority in the conditional access list.

The valid access authorities are NONE, EXECUTE (for DATASET or PROGRAM class only), READ, UPDATE, CONTROL, and ALTER. If you need more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

If you specify ACCESS and omit *access-authority*, the default value is ACCESS(READ).

If you specify the ID operand and omit both ACCESS and DELETE, the default value is ACCESS(READ).

If you specify both ACCESS and DELETE, RACF uses the last operand you specify.

DELETE
specifies that you are removing the names you identify on the ID operand from an access list for the resource. RACF deletes the names from the standard access list.

If you specify WHEN, RACF deletes the names from the conditional access list.

If you specify the ID operand and omit both ACCESS and DELETE, the default value is ACCESS(READ).

If you specify both ACCESS and DELETE, RACF uses the last operand you specify.

CLASS(*profile-name-1-class*)
specifies the name of the class to which *profile-name-1* belongs. The valid class names are DATASET and those classes defined in the class descriptor table (CDT). For a list of general resource classes defined in the IBM-supplied CDT, see Appendix B, "IBM-Supplied Resource Classes that Apply to z/VM Systems," on page 349.

If you omit CLASS, the default is DATASET.

FCLASS(*profile-name-2-class*)
specifies the name of the class to which *profile-name-2* belongs. The valid class names are DATASET and those classes defined in the class descriptor table (CDT). For a list of general resource classes defined in the IBM-supplied CDT, see Appendix B, "IBM-Supplied Resource Classes that Apply to z/VM Systems," on page 349.

If you specify FROM and omit FCLASS, RACF assumes that the class for *profile-name-2* is same as the class for *profile-name-1*. This operand is valid only when you also specify the FROM operand; otherwise, RACF ignores it.

FROM(*profile-name-2*)
specifies the name of the existing discrete or generic profile that contains the access lists RACF is to copy as the access lists for *profile-name-1*. If you specify FROM and omit FCLASS, RACF assumes that *profile-name-2* is the name of a profile in the same class as *profile-name-1*.

If *profile-name-2* contains a standard access list, RACF copies it to the profile you are changing. If *profile-name-2* contains a conditional access list, RACF copies it to the profile you are changing.

RACF modifies the access list for *profile-name-1* as follows:

- Authorizations for *profile-name-2* are added to the access list for *profile-name-1*
- If a group or user appears in both lists, RACF uses the authorization granted in *profile-name-1*
- If you specify a group or user on the ID operand and that group or user also appears in the *profile-name-2* access list, RACF uses the authorization granted on the ID operand.

To specify FROM, you must have sufficient authority to both *profile-name-1* and *profile-name-2*, as described under "Authorization Required" on page 202.

GENERIC
specifies that RACF is to treat *profile-name-1* as a generic name, even if it does not contain any generic characters. This operand is only needed if *profile-name-1* is a DATASET profile.

ID(*name ...*|*)
specifies the user IDs and/or group names of RACF-defined users or groups whose authority to access the resource you are giving, removing, or changing. If you omit this operand, RACF ignores the ACCESS and DELETE operands.

ID(*) can be used with standard or conditional access lists. You might specify ID(*) with a conditional access list, as follows:

```
PERMIT 'resource' ID(*) WHEN(PROGRAM(XYZ)) ACCESS(READ)
```

This command allows all RACF-defined users and groups READ access to the specified data set when executing program XYZ. RACF grants access to the data set, using the conditional access list, with the

authority you specify on the ACCESS operand. The value specified with ACCESS is used only if no more specific values are found. If you do not specify the ACCESS operand, or if you specify ACCESS without an access authority, RACF uses a default value of ACCESS(READ).

RESET [(ALL | STANDARD | WHEN)]

RESET | RESET(ALL)
specifies that RACF is to delete from the profile both the entire current standard access list and the entire current conditional access list.

RACF deletes both access lists before it processes any operands (ID and ACCESS or FROM) that create new entries in an access list. If you delete both access lists and specify FROM when *profile-name-2* contains two access lists, the PERMIT command copies both access lists to *profile-name-1*. In any other situation, you cannot, on one PERMIT command, add entries to both access lists.

If you specify RESET or RESET(ALL), add entries, and omit WHEN, RACF deletes both access lists, then adds entries to the standard access list.

If you specify RESET or RESET(ALL), add entries, and specify WHEN, RACF deletes both access lists, then adds entries to the conditional access list.

For profiles that include two access lists, use RESET and RESET(ALL) carefully. Unless you are copying both lists from another profile, it is a good practice to use RESET(STANDARD) to maintain the standard access list and RESET(WHEN) to maintain the conditional access list.

RESET(STANDARD)
specifies that RACF is to delete the entire current standard access list from the profile.

If you specify RESET(STANDARD) with ID and ACCESS or with FROM, RACF deletes the current standard access list from the profile before it adds the new names.

If you specify RESET(STANDARD) with ID and DELETE, RACF ignores RESET(STANDARD) and deletes only the names that you specify.

If you specify RESET(STANDARD) without ID and ACCESS, or without FROM, the resulting standard access list will be empty. An empty standard access list means that, for a general resource or a group data set profile, you must be the owner or have the SPECIAL attribute, or the profile must be within the scope of a group in which you have the group-SPECIAL attribute, in order to update the access list again.

For a DATASET profile, an empty conditional access list means that no users or groups can access the data set by executing a program.

RESET(WHEN)
RESET(WHEN) specifies that RACF is to delete the entire current conditional access list from the profile.

If you specify RESET(WHEN) with ID and ACCESS or with FROM, RACF deletes the current conditional access list from the profile before it adds the new names.

If you specify RESET(WHEN) with ID, DELETE, and WHEN, RACF ignores RESET(WHEN) and deletes only the names that you specify.

If you specify RESET(WHEN) without ID and ACCESS, or without FROM, the resulting conditional access list will be empty.

WHEN(TERMINAL(*terminal-id ...*))
specifies that the indicated users or groups have the specific access authority when logged on to the named terminal.

Examples

Example 6

Operation: User WJE10 wants to give UPDATE access authority to z/VM minidisk USERA.195 to all the users in the group RESEARCH. z/VM minidisk USERA.195 is protected by a discrete profile.

Known: User WJE10 and group RESEARCH are RACF-defined. z/VM minidisk USERA.195 is RACF-defined.

Command:
```
PERMIT USERA.195 CLASS(VMMDISK) ID(RESEARCH)
ACCESS(UPDATE)
```

Defaults: None

Example 7

Operation: User ADM1 wants to delete the existing standard access list from the discrete profile protecting the z/VM minidisk EUROPE.19E, then copy the standard access list from the discrete profile GROUP.193 to the discrete profile for EUROPE.19E.

Known: User ADM1 has the SPECIAL attribute. EUROPE.19E is in the VMMDISK class.

Command:
```
PERMIT EUROPE.19E CLASS(VMMDISK) FROM
('GROUP.193') RESET(STANDARD)
```

Defaults: FCLASS(VMMDISK)

Example 8

Operation: User ADM1 wants to replace the conditional access list in the discrete profile that protects the minidisk MAINT.191. Two users, SYSPROG1 and SYSPROG2, are to be allowed to update the minidisk when they are using the terminal named TERM001.

Known: User ADM1 has the SPECIAL attribute. MAINT.191 is a profile in the VMMDISK class. TERM001 is a profile in the TERMINAL class. Users SYSPROG1 and SYSPROG2 are defined to RACF.

Command:
```
PERMIT MAINT.191 CLASS(VMMDISK) RESET(WHEN)
ID(SYSPROG1 SYSPROG2) ACCESS(UPDATE)
WHEN(TERMINAL(TERM001))
```

Defaults: None

RAC (Enter RACF Commands on z/VM)

System environment

This command applies to z/VM systems only and cannot be issued from a RACF service machine.

Purpose

Use the RAC command processor to enter RACF commands from a CMS command line on z/VM systems. To enter a RACF command, precede the command with RAC. Any noninteractive RACF command can be used with RAC.

The output from the RACF command will be captured and saved to a file called RACF DATA on the user's specified disk or directory.

For additional usage information, see *z/VM: RACF Security Server System Programmer's Guide*.

Attention:
The INACTIVE operand of the RVARY command is not recommended for use with RAC. In a non-SSI cluster environment, the RACF command session should be used instead. For an explanation of the issues involved, see the descriptions for messages RPIRAC009W and RPIRAC010W.

Related Commands

Use the RACF command to enter a RACF command session on z/VM.

Authorization Required

If your installation has decided to restrict access to the RAC command, you may not be able to use the RAC command; contact your security administrator to be given access. You must have at least READ access to the resource named 'RAC' in the VMCMD class.

Syntax

The complete syntax of the RAC command processor is:

```
RAC                    RACF-command
```

Parameters

RACF-command
specifies any noninteractive RACF command.

No prompting is done if a required keyword is missing or misspelled. RAC terminates the command.

RAC captures the output from the command and places it in a file called RACF DATA on the user's specified disk or directory (file mode A is the default).

RACF-command cannot be SMF or BLKUPD. BLKUPD can be entered by authorized users during a RACF command session.

Comments

If you need to enter a command that is longer than the z/VM command line, you may choose one of the following methods.

- You may write an exec similar to the one following.

```
/* */
trace "o"
cmd = "adduser ewing data('This is a sample of a large amount"
cmd = cmd||" of installation data that exceeds the command line"
cmd = cmd||" limit of one hundred thirty characters of any"
cmd = cmd||" information that the user would like to enter')"
rac cmd
```

- To enter the command interactively, issue the RAC command with no operands. The RAC exec will prompt you to enter command data. Keep entering lines of the RACF command until you are finished. Next, enter a null line. The RAC command processor will send the complete command to the RACF service machine for processing.

  When you enter a RACF command using the above method, the RAC exec accepts your input exactly as is. Remember to enter spaces at the end of a given line of input if necessary.

Up to 3500 characters will be accepted by the RAC command processor. If this limit is exceeded, you will receive an error message.

See *z/VM: RACF Security Server System Programmer's Guide* for more information.

The RAC command is an application that uses the SMSG communication protocol. If RAC is used within an application, that application should not use SMSG. ALL SMSGs received while the RAC command is processing a request to the RACF service machine are written to the RACF DATA file.

You can also group several RAC commands in an exec.

```
/* SHORT EXEC FOR SIMPLE RAC COMMANDS */

'RAC AU USERTEST'
'RAC RDEFINE VMMDISK USERTEST.191 APPLDATA("TESTING EXEC")'
'RAC RLIST VMMDISK USERTEST.191 ALL'
'RAC RDELETE VMMDISK USERTEST.191'
'RAC DELUSER USERTEST'
```

If you are using multiple RACF service machines, refer to “Comments” on page 209.

Comments

A user can modify RAC's processing by changing global variables with the GLOBALV command of CMS. The user can specify:

- Whether the RACF DATA file is appended with the RACF command output or replaced by that output each time RAC is used
- The file mode of the RACF DATA file
- The amount of time RAC waits for a response from the RACF server.
- The user ID of the service machine the command should be sent to.
- Whether duplicate output from propagated commands is listed to the user's terminal

The user can make these changes by specifying `GLOBALV SELECT $RACGRP` with one of the following GLOBALV variables.

For further information on tailoring RAC for your installation, see *z/VM: RACF Security Server System Programmer's Guide*.

$RAC_APN N | Y
: controls whether RAC appends RACF command output to the file RACF DATA or replaces RACF DATA with the new output. The default value is `N`, meaning the RACF DATA file will be replaced with the new RACF command output each time RAC is used. If you specify `Y`, the RACF command output will be appended to RACF DATA. No RACF command output will be displayed at the user's terminal.

$RAC_FLE A | filemode of disk or directory with R/W access
: specifies the file mode of the RACF DATA file. The default is file mode A. The user **must** have WRITE access to the file mode specified.

$RAC_ISPF N | Y
controls whether RACF output to the terminal screen is suppressed. The default (N) specifies that output should go to the terminal screen and to the RACF DATA file. When this variable is set to Y, RACF output is sent only to the RACF DATA file.

Note: This variable is always reset to the default (N) upon exiting the RACF ISPF panels.

$RAC_TIM *minutes*
specifies the number of minutes RAC is to wait for a response from the RACF server before terminating. Valid values for *minutes* are 1 through 9. The default is 1.

Long-running commands (such as SEARCH) may take a long time to respond to the user with output. Changing *minutes* allows more time for the RACF server to respond.

$RAC_SRV *RACF-service-machine-userID*
in an environment of multiple RACF service machines, $RAC_SRV indicates which service machine the RACF command should be sent to. If you do not specify a value, the command is sent to the RACF service machine that was assigned to your user ID at LOGON. See "Comments" on page 209 for more information.

$RAC_SSI N | Y
controls whether the RACOUTP EXEC displays all the output from propagated commands. $RAC_SSI N is the default and will result in the output from the original server being displayed and any output from propagated commands that differs from the original being displayed. $RAC_SSI Y is the verbose setting so that all the returned output is listed to the user's terminal.

If you want to check the settings of your global variables, enter `GLOBALV SELECT $RACGRP LIST`.

If the variables you enter are not acceptable, the defaults are in control.

Comments

RACF automatically propagates the RVARY command to all RACF servers that run on the same z/VM system, and to all RACF servers that run on other systems in the same SSI cluster as the issuing system. RACF does not automatically propagate the RVARY command to z/VM systems that share the RACF database outside of an SSI cluster. You must issue the RVARY command separately for each system or restart the RACF servers on the other system or IPL the other system.

Examples

Example 1

Operation	A user wants to list her RACF user profile using the RAC command.
Known	The user has not changed any of the GLOBALV variables.
Command	`RAC LISTUSER`
Defaults	$RAC_APN = N; $RAC_FLE = A; $RAC_TIM = 1
Results	The user's RACF profile is displayed at her terminal and is also saved to file RACF DATA A.

Example 2

Operation	User SUSIE wants the output of RACF commands appended to the RACF DATA file and also to change the file mode to B.
Known	$RAC_APN is used to tell whether RACF DATA is appended. $RAC_FLE specifies the file mode of the RACF DATA file.
Command	`GLOBALV SELECT $RACGRP SET $RAC_APN Y` `GLOBALV SELECT $RACGRP SET $RAC_FLE B`
Results	RACF DATA will now be appended instead of replaced and will be on the disk or directory accessed as B.

Example 3

Operation User ECOSTELL wants to list the RAC global variables.

Known The selector for the RAC global variables is $RACGRP. ECOSTELL has changed the filemode for RACF DATA to B. RACF DATA is to be appended each time RAC is called. The time out value has been set to 3.

Command `GLOBALV SELECT $racgrp LIST`

Output

```
SELECTED TABLE IS: $RACGRP
 $RAC_TIM=3
 $RAC_APN=Y
 $RAC_FLE=B
```

RACF (Begin RACF Command Session on z/VM)

System environment

This command applies to z/VM systems only and cannot be issued from a RACF service machine.

Purpose

Use the RACF command to begin a RACF command session on z/VM.

After you enter a RACF command session, you can issue other RACF commands for which you are authorized.

Note:

1. In an SSI cluster, the RVARY, SETROPTS, and SETEVENT commands are propagated to other SSI members in a RACF command session. All output from these members is displayed in the session.
2. It is recommended that general users enter RACF commands with the RAC command processor. See "RAC (Enter RACF Commands on z/VM)" on page 207.
3. To end a RACF command session, use the END command as described in "END (End RACF Command Session on z/VM)" on page 145.
4. RACF does not require you to enter a password or password phrase to establish a RACF environment. Your installation, however, may require it. If your installation requires a password or password phrase, RACF prompts you for your logon password or password phrase. You can change your password or password phrase when the prompt appears; if you are then denied access because your installation has restricted usage of RACF, your password or password phrase change is still in effect. After you have entered your password or password phrase, you can issue the RACF commands for which you have sufficient authority.
5. A RACF command session does not support omitting the file pool ID from SFS file and directory profile names. For more information, see "Default Naming Conventions" on page 343.

Authorization Required

If your installation has decided to restrict access to the RACF command, you may not be able to use the RACF command; contact your security administrator to be given access. You must have at least READ access to the resource named 'RACF' in the VMCMD class.

Syntax

The complete syntax of the RACF command is:

```
RACF                    [ (BATCH) | (PANEL ]
```

Parameters

(BATCH
specifies that, during a RACF command session, you do not want to receive a prompting message if you make an error when entering a RACF command. RACF will issue an error message but no prompting message, after which you must reenter the entire command.

(PANEL
invokes the ISPF panels for RACF.

Comments

If you specify BATCH for a command session and during the session you enter a RACF command with a misspelled operand as follows:

```
HELP ALTUSER ALLL
```

RACF responds with the following error messages but does not issue a prompting message:

```
IKJ56712I INVALID KEYWORD, ALLL
RPITMP003E RACF CMND ERROR
```

You must then reenter the entire command correctly as follows:

```
HELP ALTUSER ALL
```

If you do not specify BATCH, RACF issues a prompting message as well as an error message. For example, if you do not specify BATCH and during a command session you enter a RACF command with a misspelled operand as follows:

```
HELP ALTUSER ALLL
```

RACF responds with the following error and prompting messages:

```
IKJ56712I INVALID KEYWORD, ALLL
IKJ56703A REENTER THIS OPERAND
```

You can then reenter only that part of the command that is in error; in the example, you would reenter ALL.

You can also choose to escape from the REENTER prompt:

1. Type HX and press Enter.
2. When you get a READY prompt, type hx and press Enter again.

You can then either continue the RACF command session, or type END and press Enter to exit the RACF command session.

```
/* short exec for simple RACF commands */

PUSH 'END'
PUSH 'DELUSER USERTEST'
PUSH 'RDELETE VMMDISK USERTEST.191'
PUSH 'RLIST VMMDISK USERTEST.191 ALL'
PUSH 'RDEFINE VMMDISK USERTEST.191 APPLDATA ("TESTING EXEC")'
PUSH 'AU USERTEST'
'RACF (BATCH'
EXIT
```

If password prompting is in effect, you can put the password in when you enter a RACF session. For example,

```
'RACF 999999 (BATCH'
```

RALTER (Alter General Resource Profile)

System environment

Purpose

Use the RALTER command to:

- Alter the profile for one or more resources belonging to classes defined in the class descriptor table
- Change the global access checking table
- Change the list of security categories
- Change the list of security levels.

To have changes take effect after altering a generic profile if the class is not RACLISTed by SETROPTS RACLIST, one of the following steps is required:

- The security administrator issues the SETROPTS command:

  ```
  SETROPTS GENERIC(class-name) REFRESH
  ```

  See the SETROPTS command for authorization requirements.
- The user of the resource logs off and logs on again.

To have changes take effect after altering a generic profile if the class is RACLISTed, the security administrator issues the following command:

```
SETROPTS RACLIST(class-name) REFRESH
```

For more information, refer to *z/VM: RACF Security Server Security Administrator's Guide*.

Related Commands

- To define a general resource profile, use the RDEFINE command as described in "RDEFINE (Define General Resource Profile)" on page 225.
- To list a general resource profile, use the RLIST command as described in "RLIST (List General Resource Profile)" on page 248.
- To permit or deny access to a general resource profile, use the PERMIT command as described in "PERMIT (Maintain Resource Access Lists)" on page 202.

Authorization Required

To alter the profile for a resource belonging to a class defined in the class descriptor table, you must have sufficient authority over the resource. RACF makes the following checks until one of the conditions is met:

- You have the SPECIAL attribute.
- The resource profile is within the scope of a group in which you have the group-SPECIAL attribute.
- You are the owner of the profile.
- To assign a security label, you must have the SPECIAL attribute or have READ access to the security label profile. However, the security administrator can limit the ability to assign security labels to only users with the SPECIAL attribute.
- To assign a security category to a profile, you must have the SPECIAL attribute, or the access category must be in your user profile.
- To assign a security level to a profile, you must have the SPECIAL attribute, or, in your own profile, a security level that is equal to or greater than the security level you are assigning.

- To modify the SSIGNON segment, your installation must permit you to do so through field level access checking.

For discrete profiles in classes other than VMMDISK:

- You are on the access list for the resource and you have ALTER authority. If you have any other level of authority, you cannot use the command for this resource.
- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is in the access list and has ALTER authority.
- The universal access authority for the resource is ALTER.

For both discrete and generic profiles, when you specify the GLOBALAUDIT operand:

- You have the AUDITOR attribute or the profile is within the scope of a group in which you have group-AUDITOR attribute.

The following operands have restrictions noted with the description of each operand:

- ADDMEM
- DELMEM
- GLOBALAUDIT

Syntax

The complete syntax of the command is:

```
RALTER          ***class-name***
RALT            (***profile-name ...***)
                [ ADDCATEGORY(category-name ...)
                | DELCATEGORY[( {category-name...| *})] ]
                [ {ADDMEM | DELMEM} (member ...) ]
                [ APPLDATA('application-data') | NOAPPLDATA ]
                [ AUDIT( access-attempt [(audit-access-level)] ...) ]
                [ DATA('installation-defined-data') | NODATA ]
                [ GLOBALAUDIT(access-attempt [(audit-access-level)] ...) ]
                [ LEVEL(nn) ]
                [ NOTIFY [(userid)] | NONOTIFY ]
                [ OWNER(userid or group-name) ]
                [ SECLABEL(seclabel-name ...) | NOSECLABEL ]
                [ SECLEVEL(seclevel-name ...) | NOSECLEVEL ]
                [ SESSION(
                  [ INTERVAL(n) | NOINTERVAL ]
                  [ LOCK | NOLOCK ]
                  [ SESSKEY(session-key) | NOSESSKEY ]
                  )
                | NOSESSION} ]
                [ SSIGNON(
                  [ KEYMASKED(key-value)
                  | KEYENCRYPTED(key-value)]) ]
                [ TIMEZONE( {E | W} hh[.mm]) | NOTIMEZONE ]
                [ UACC(access authority) ]
                [ WARNING | NOWARNING ]
                [ WHEN( [DAYS(day-info)] [TIME(time-info)] ) ]
```

Parameters

class-name
specifies the name of the class to which the resource belongs. Valid class names are those defined in the IBM-supplied class descriptor table or in the installation-defined class descriptor table. For a list of general resource classes supplied by IBM, see Appendix B, "IBM-Supplied Resource Classes that Apply to z/VM Systems," on page 349.

This operand is required and must be the first operand following RALTER.

(*profile-name ...*)
specifies the name of the profile you want to change. The name you specify must be the name of an existing discrete or generic profile in the specified class. RACF uses the class descriptor table (CDT) to determine the syntax of resource names within the class.

This operand is required and must be the second operand following RALTER.

- If you specify more than one *profile-name*, you must enclose the list of names in parentheses.
- If you specify *class-name* as GLOBAL, *profile-name* must be either DATASET or a valid class name (other than a resource grouping class) as specified in the CDT. If you specify *class-name* as GLOBAL or SECDATA and also specify ADDMEM or DELMEM, you can specify only one value for *profile-name*.

Note: RACF processes each resource you specify independently, and all operands you specify apply to each named resource. If an error occurs while processing a resource, RACF issues a message and continues processing with the next resource.

ADDCATEGORY | DELCATEGORY

ADDCATEGORY(*category-name ...*)
specifies one or more names of installation-defined security categories. The *category-name* you specify must be defined as members of the CATEGORY profile in the SECDATA class. (For information on defining security categories, see the *z/VM: RACF Security Server Security Administrator's Guide*.)

Specifying ADDCATEGORY causes RACF to add any *category-names* you specify to any list of required categories that already exists in the resource profile. All users previously allowed to access the resource can continue to do so only if their profiles also include the additional values for *category-names*.

When the SECDATA class is active and you specify ADDCATEGORY, RACF performs security category checking in addition to its other authorization checking. If a user requests access to a resource, RACF compares the list of security categories in the user profile with the list of security categories in the resource profile. If RACF finds any security category in the resource profile that is not in the user's profile, RACF denies access to the resource. If the user's profile contains all the required security categories, RACF continues with other authorization checking.

When the SECDATA class is not active, RACF ignores this operand. When the CATEGORY profile does not include a member for *category-name*, you are prompted to provide a valid category name.

DELCATEGORY[(*category-name ...*|*)]
specifies one or more names of installation-defined security categories you want to delete from the resource profile. Specifying an asterisk (*) deletes all categories; RACF no longer performs security category checking for the resource.

Specifying DELCATEGORY by itself causes RACF to delete from the profile only undefined category names (those category names that were once known to RACF but that the installation has since deleted from the CATEGORY profile.)

When the SECDATA class is not active, RACF ignores *category-name*. When the CATEGORY profile does not include a member for a *category-name*, you are prompted to provide a valid *category-name*.

ADDMEM | DELMEM

ADDMEM(*member....*)
specifies the resource names that RACF is to add to the members of the resource group indicated by *profile-name*.

To add members using the RALTER command, you need one of the following authorities, in addition to the authority needed to issue the RALTER command:

1. For classes other than PROGRAM, SECDATA, GLOBAL, RACFVARS, NODES, and VMXEVENT, if the member resources are already RACF-protected by a member class profile or as a member of a profile in the same grouping class, one of the following must be true:
   - You have ALTER access authority to the member.
   - You are the owner of the member resource.
   - The member resource is within the scope of a group in which you have the group-SPECIAL attribute.
   - You have the SPECIAL attribute.
2. For classes other than PROGRAM, SECDATA, GLOBAL, RACFVARS, NODES, and VMXEVENT, if the member resources are not RACF-protected (that is, there is no profile defined for that member), one of the following must be true:
   - You have CLAUTH authority to define resources in the member resource class.
   - You have the SPECIAL attribute.
3. To add a member to a profile in the RACFVARS or NODES class, one of the following must be true:
   - You have CLAUTH authority to define resources in the specified class (for example, RACFVARS or NODES).
   - You have the SPECIAL attribute.
   - You are the owner of the profile indicated by *profile-name*.
   - You have ALTER access authority to the profile indicated by *profile-name*.
4. To add a member to a profile in the PROGRAM or SECDATA class, one of the following must be true:
   - You have CLAUTH authority to define resources in the specified class (for example, PROGRAM or SECDATA).
   - You have the SPECIAL attribute.
5. To add a member to a profile in the GLOBAL class (other than the GLOBAL FILE, GLOBAL DIRECTRY, or GLOBAL DATASET profile) where the syntax is:

   ```
   RALT GLOBAL class-name ADDMEM(resource-name/access-level)
   ```

   one of the following must be true:
   - If the profile *resource-name* is already RACF-protected by a profile in class *class-name*:
     - You have ALTER access authority to the profile *resource-name* in class *class-name*.
     - You are the OWNER of the profile *resource-name*.
     - The profile *resource-name* in class *class-name* is within the scope of a group in which you have the group-special attribute.
     - You have the SPECIAL attribute.
   - If the profile *resource-name* is not already RACF-protected (that is, there is no profile defined for that member in class *class-name*):
     - You have CLAUTH authority to define resources in the class *class-name*.
     - You have the SPECIAL attribute.

6. To add a member to the GLOBAL DATASET profile, one of the following must be true:
   - You are the owner of the DATASET profile in the GLOBAL class.
   - The member is within the scope of a group in which you have the group-SPECIAL attribute, or the high-level qualifier of the member name is your user ID.
   - You have the SPECIAL attribute.
7. To add a member to the GLOBAL DIRECTRY or GLOBAL FILE profile, you need no additional authority.
8. To add a member to a profile in the VMXEVENT class, the following rules apply:
   - To set the control options (add a member specifying /CTL or /NOCTL), you must have the SPECIAL attribute.
   - To set the audit options (add a member specifying /AUDIT), you must have the AUDITOR attribute.

For more information on ADDMEM, see Specifying member on the ADDMEM operand.

DELMEM(*member*....)
specifies the resource names that are to be deleted from the resource group indicated by *profile-name*. This operand is ignored if the class name specified is not a resource group class.

If *class-name* is specified as GLOBAL, VMXEVENT, or PROGRAM, the rules for "member" are the same as given for ADDMEM. If *class-name* is specified as SECDATA, "member" should be a valid seclevel name or category name.

To delete a member from a profile in the VMXEVENT class, the following rules apply:

- To delete a member specifying /CTL or /NOCTL, you must have the SPECIAL attribute.
- To delete a member specifying /AUDIT, you must have the AUDITOR attribute.

APPLDATA | NOAPPLDATA

APPLDATA('*application-data*')
specifies a text string that will be associated with each of the named resources. The text string may contain a maximum of 255 characters and must be enclosed in single quotation marks. The text string may contain DCBS data.

This information, if present, can be displayed with the RLIST command and will be included in the resident profile generated by RACLIST.

Note: For the TIMS and GIMS class, specify *application-data* as REVERIFY to force the user to reenter his password whenever the transaction or transactions listed in the *profile-name* or ADDMEM operands are used.

NOAPPLDATA
specifies that the RALTER command is to delete the text string that was present in the profile associated with the resource.

AUDIT(*access-attempts*[(*audit-access-level*)])

access-attempts
specifies which access attempts you want to log on the SMF data set for the SMF data file for z/VM. The following options are available:

ALL
specifies that you want to log both authorized accesses and detected unauthorized attempts to access the resource.

FAILURES
specifies that you want to log detected unauthorized attempts to access the resource.

NONE
specifies that you do not want any logging to be done for accesses to the resource.

SUCCESS
specifies that you want to log authorized accesses to the resource.

audit-access-level
specifies which access levels you want to log on the SMF data set for the SMF data file for z/VM. The levels you can specify are:

ALTER
logs ALTER access-level attempts only.

CONTROL
logs access attempts at the CONTROL and ALTER levels.

READ
logs access attempts at any level. This is the default value if no access level is specified.

UPDATE
logs access attempts at the UPDATE, CONTROL, and ALTER levels.

You cannot audit access attempts at the EXECUTE level.

DATA | NODATA

DATA('*installation-defined-data*')
specifies up to 255 characters of installation-defined data to be stored in the profile for the resource. The data must be enclosed in single quotation marks.

This information is listed by the RLIST command. It is also available to RACF postprocessing installation exit routines for RACHECK (for resources belonging to classes defined in the class descriptor table) or RACINIT (for APPL and TERMINAL) SVCs.

NODATA
specifies that the RALTER command is to delete the installation-defined data in the resource profile.

GLOBALAUDIT
specifies which access attempts the user who has the AUDITOR attribute wants to log on the SMF data set for the SMF data file for z/VM. The options (ALL, SUCCESS, FAILURES, and NONE) and the *audit-access-level* values are the same as described for AUDIT.

To use GLOBALAUDIT, you must have the AUDITOR attribute, or the resource profile must be within the scope of a group in which you have the group-AUDITOR attribute.

Regardless of the value you specify for GLOBALAUDIT, RACF always logs all access attempts specified on AUDIT.

LEVEL(*nn*)
specifies a level indicator, where *nn* is an integer between 00 and 99. Your installation assigns the meaning of the value. It is available to RACF postprocessing installation exit routines for RACHECK (for resources belonging to classes defined in the class descriptor table) or RACINIT (for APPL and TERMINAL) SVCs. It is included on all records that log resource accesses and is listed by the RLIST command.

NOTIFY | NONOTIFY

NOTIFY[(*userid*)]
specifies the user ID of a RACF-defined user to be notified whenever RACF uses this profile to deny access to a resource. If you specify NOTIFY without specifying a user ID, RACF takes your user ID as the default; you will be notified whenever the profile denies access to a resource.

A user who is to receive NOTIFY messages should log on frequently to take action in response to the unauthorized access attempt described in each message. RACF sends NOTIFY messages as follows:

- On z/VM, RACF sends NOTIFY messages to the specified user ID. (Note that you should not specify the user ID of a virtual machine that always runs disconnected.) If the user ID is logged on, the message immediately appears on the user's screen. If the user ID is not logged on or is

disconnected, RACF sends the message to the user in a reader file. The name of this reader file will be the user ID specified on the NOTIFY keyword and the type will be NOTIFY.

When the resource profile also includes WARNING, RACF might have granted access to the resource to the user identified in the message.

When RACF denies access to a resource, it does **not** notify a user:

- When the resource is in the PROGRAM class.
- When the resource is in a class for which your installation has built in-storage profiles using the RACLIST macro. Profiles built using the RACLIST macro are made resident by certain resource managers such as IMS and CICS so that they can be used by the FRACHECK facility for authorization checking. FRACHECK does not issue NOTIFY messages.

NONOTIFY
specifies that no user is to be notified when RACF uses this profile to deny access to a resource.

OWNER(*userid* or *group-name*)
specifies a RACF-defined user or group to be assigned as the new owner of the resource you are changing.

To change the owner of a resource, you must be the current owner of the resource or have the SPECIAL attribute, or the profile must be within the scope of a group in which you have the group-SPECIAL attribute. The user specified as the owner does not automatically have access to the resource. Use the PERMIT command to add the owner to the access list as desired.

SECLABEL | NOSECLABEL

SECLABEL(*seclabel-name*)
specifies an installation-defined security label for this profile. A security label corresponds to a particular security level (such as CONFIDENTIAL) with a set of zero or more security categories (such as PAYROLL or PERSONNEL).

For a list of security labels that you are authorized to use, enter:

```
SEARCH CLASS(SECLABEL)
```

If you are authorized to use the SECLABEL, RACF stores the name of the security label you specify in the resource profile.

If you are not authorized to the SECLABEL or if the name you had specified is not defined as a SECLABEL profile in the SECLABEL class, the resource profile is not created. If the SECLABEL class is active and the security level is specified in this profile, any security levels and categories in the profile are ignored.

NOSECLABEL
removes the security label, if one had been specified, from the profile.

SECLEVEL | NOSECLEVEL

SECLEVEL(*seclevel-name*)
specifies the name of an installation-defined security level. This name corresponds to the number that is the minimum security level that a user must have to access the resource. The variable *seclevel-name* must be a member of the SECLEVEL profile in the SECDATA class.

When you specify SECLEVEL and the SECDATA class is active, RACF adds security level access checking to its other authorization checking. If global access checking does not grant access, RACF compares the security level allowed in the user profile with the security level required in the resource profile. If the security level in the user profile is less than the security level in the resource profile, RACF denies the access. If the security level in the user profile is equal to or greater than the security level in the resource profile, RACF continues with other authorization checking. RACF does not perform security level checking when the resource whose profile you are changing is in the PROGRAM class.

If the SECDATA class is not active, RACF stores the name you specify in the resource profile. When the SECDATA class is activated and the name you specified is defined as a SECLEVEL profile, RACF can perform security level access checking for the resource profile. If the name you specify is not defined as a SECLEVEL profile, you are prompted to provide a valid *seclevel-name*.

NOSECLEVEL
specifies that the RALTER command is to delete the security level name from the profile. RACF no longer performs security level checking for the resource.

SESSION | NOSESSION

SESSION
controls the establishment of sessions between logical units under LU6.2. This operand is only valid for the APPCLU resource class. It allows the following suboperands to add, change, or delete SESSION segment field values when changing an APPCLU class profile.

INTERVAL(*n*) | NOINTERVAL

INTERVAL(*n*)
sets the maximum number of days the session key is valid. This number, *n*, is in the range of 1 to 32767. If the key interval is longer than the installation maximum (set with SETROPTS SESSIONINTERVAL), the INTERVAL will not be changed.

NOINTERVAL
There is no limit on the number of days the key is valid.

LOCK | NOLOCK

LOCK
marks the profile as locked.

NOLOCK
unlocks a previously locked profile.

SESSKEY | NOSESSKEY

SESSKEY(*session-key*)
changes the key for this profile. *Session key* can be expressed in two ways:

- x'y' where y is a 1-to-16-digit hexadecimal number
- z or 'z' where z is a 1-to-8-character string.

Note: If the entire 16 digits or 8 characters are not used, the field is padded to the right with binary zeros.

NOSESSKEY
deletes the session key for this profile

NOSESSION
deletes the SESSION segment from this profile.

SSIGNON(KEYMASKED(*key-value*)|(KEYENCRYPTED(*key-value*))
defines the secured signon application key and indicates the method you want to use to protect the key value within the RACF database on the host. You can mask or encrypt the key. The *key-value* represents a 64-bit (8-byte) key that must be represented as 16 hexadecimal characters. The valid characters are 0 through 9 and A through F.

Note:

1. As with RACF passwords, the database unload facility does not unload secured signon application keys.
2. The RLIST command does not list the value of the secured signon application keys. Therefore, when you define the keys, you should note the value and keep it in a secure place.
3. These operands can be specified only via the RACF commands; they are not available in the ISPF panels.

KEYMASKED(*key-value*)
indicates that you want to mask the key value using the masking algorithm.

Note:

1. You can specify this operand only once for each application key.
2. If you mask a key, you *cannot* encrypt it. These are mutually exclusive.

You can use the RLIST command described in "RLIST (List General Resource Profile)" on page 248 to be sure the key is protected.

KEYENCRYPTED(*key-value*)
indicates that you want to encrypt the key value.

Note:

1. You can specify this operand only once for each application key.
2. If you encrypt a key, you *cannot* mask it. These are mutually exclusive.
3. A cryptographic product must be installed and active on the system.

You can use the RLIST command described in "RLIST (List General Resource Profile)" on page 248 to be sure the key is protected.

TIMEZONE | NOTIMEZONE

TIMEZONE({E|W} *hh*[*.mm*])
specifies the time zone in which a terminal resides. TIMEZONE is valid only for resources in the TERMINAL class; RACF ignores it for all other resources.

Specify TIMEZONE only when the terminal is not in the same time zone as the processor on which RACF is running. In this situation, TIMEZONE provides the information RACF needs to calculate the time and day values correctly. If you identify more than one terminal in the *profile-name* operand, all the terminals must be in the same time zone.

On TIMEZONE, you specify whether the terminal is east (E) or west (W) of the system and by how many hours (hh) and, optionally, minutes (mm). The terminal time zone is different from the processor time zone. Valid hour values are 0 through 11, and valid minute values are 00 through 59.

For example, if the processor is in New York and the terminal is in Los Angeles, specify TIMEZONE(W 3). If the processor is in Houston and the terminal is in New York, specify TIMEZONE(E 1).

If you change the local time on the processor (to accommodate daylight savings time, for instance), RACF adjusts its time calculations accordingly. If, however, the processor time zone and the terminal time zone do not change in the same way, you must adjust the terminal time zones yourself, as described for the WHEN(TIME) operand.

NOTIMEZONE
specifies that the terminal is in the same time zone as the processor. NOTIMEZONE is valid only for resources in the terminal class; RACF ignores it for all other resources.

UACC(*access-authority*)
specifies the universal access authority to be associated with this resource. The universal access authorities are ALTER, CONTROL, UPDATE, READ, EXECUTE (for controlled programs only), and NONE.

Note:

1. For the VMBATCH class, a user ID requires CONTROL access authority to be able to operate as an alternate user ID.
2. See "Access Authority for Minidisks on z/VM" on page 12 for more information.
3. For all other resources listed in the class descriptor table, RACF treats CONTROL and UPDATE authority as READ authority.

WARNING | NOWARNING

WARNING
specifies that, even if access authority is insufficient, RACF is to issue a warning message and allow access to the resource. However, z/VM CP initiated requests (for example, LINK commands) are either deferred to CP or rejected, depending on the configuration of the SYSSEC macro. For information about the SYSSEC macro, see *z/VM: RACF Security Server Macros and Interfaces*. RACF also records the access attempt in the SMF record if logging is specified in the profile. RACF does **not** issue a warning message for a resource when the resource is:

- In the PROGRAM class
- In a class for which your installation has built in-storage profiles using the RACLIST macro. Profiles built using the RACLIST macro are made resident by certain resource managers such as IMS and CICS so that they can be used by the FRACHECK facility for authorization checking. FRACHECK does not issue WARNING messages.

NOWARNING
specifies that if access authority is insufficient, RACF is to deny the user access to the resource and not issue a warning message.

WHEN([DAYS(*day-info*)][TIME(*time-info*)])
specifies, for resources in the TERMINAL class, the days of the week or the hours in the day when the terminal can be used to access the system. The day-of-week and time restrictions apply only when a user logs on to the system; that is, RACF does not force the user off the system if the end-time occurs while the user is logged on.

If you specify the WHEN operand, you can restrict the use of the terminal to certain days of the week or to a certain time period on each day. You can also restrict access to both certain days of the week and to a certain time period within each day.

To allow use of the terminal only on certain days, specify DAYS(*day-info*), where *day-info* can be any one of the following:

ANYDAY
allows use of the terminal on any day.

WEEKDAYS
allows use of the terminal only on weekdays (Monday through Friday).

***day*...**
allows use of the terminal only on the days specified, where *day* can be MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, or SUNDAY, and you can specify the days in any order.

To allow use of the terminal only during a certain time period of each day, specify TIME(*time-info*), where *time-info* can be any one of the following:

ANYTIME
RACF allows use of the terminal at any time.

start-time*:*end-time
RACF allows use of the terminal only during the specified time period. The format of both start-time and end-time is *hhmm*, where *hh* is the hour in 24-hour notation (00 through 24) and *mm* is the minutes (00 through 59) within the range 0001 - 2400. Note that 2400 indicates 12:00 a.m. (midnight).

If *start-time* is greater than *end-time*, the interval spans midnight and extends into the following day.

Specifying *start-time* and *end-time* is straightforward when the processor on which RACF is running and the terminal are in the same time zone; you specify the time values in local time.

If, however, the terminal is in a different time zone from the processor and you want to restrict access to certain time periods, you have two choices. You can specify the TIMEZONE operand to allow RACF to calculate the time and day values correctly. Or, you can adjust the time values

yourself, by translating the *start-time* and *end-time* for the terminal to the equivalent local time for the processor.

For example, assume that the processor is in New York and the terminal is in Los Angeles, and you want to allow access to the terminal from 8:00 A.M. to 5:00 P.M. in Los Angeles. In this situation, you would specify TIME(1100:2000). If the processor is in Houston and the terminal is in New York, you would specify TIME(0900:1800).

If you omit DAYS and specify TIME, the time restriction applies to any day-of-week restriction already specified in the profile. If you omit TIME and specify DAYS, the days restriction applies to any time restriction already specified in the profile. If you specify both DAYS and TIME, RACF allows use of the terminal only during the specified time period and only on the specified days.

Examples

Example 1

Operation: User TRA02 wants to change the owner and universal access for terminal TERMID01 and restrict use of the terminal to weekdays during regular business hours (8:00 A.M. to 6:00 P.M.).

Known: User TRA02 has the SPECIAL attribute. Terminal TERMID01 is defined to RACF. Terminal TERMID01 is in the same time zone as the processor on which RACF is running.

Command:
```
RALTER TERMINAL TERMID01 OWNER(TRA02)
UACC(ALTER) WHEN(DAYS(WEEKDAYS)TIME(0800:1800))
```

Defaults: None

Example 2

Operation: User RFF23 wants to delete the two data fields associated with the terminal T3E8. The user wants to be notified whenever the terminal profile denies access to the terminal.

Known: User RFF23, who is a RACF-defined user, is the owner of the T3E8 terminal entry.

Command:
```
RALTER TERMINAL T3E8 NODATA NOAPPLDATA
NOTIFY(RFF23)
```

Defaults: None

Example 3

Operation: User ADM1 wants to delete the data fields associated with the generic profile * in the TERMINAL class.

Known: User ADM1 has the SPECIAL attribute.

Command:
```
RALTER TERMINAL * NODATA NOAPPLDATA
```

Defaults: None

Example 4

Operation: User PAYADM1 wants to add the PAYROLL category to the list of security categories known to RACF.

Known: User PAYADM1 has the SPECIAL attribute. RACF security category checking is active.

Command:
```
RALTER SECDATA CATEGORY ADDMEM(PAYROLL)
```

Defaults: None

Example 5

Operation: The security administrator wants to change the key value of a profile in the PTKTDATA class so the value becomes encrypted.

Known: NONNEL is the user ID of the security administrator.

The profile name is TSOR004.

The *key-value* is B004194019641980.

Command:
```
RALTER PTKTDATA TSOR004
SSIGNON(KEYENCRYPTED(B004194019641980))
```

Defaults: None

Example 6

Operation: User SECADM wants to change the universal access authority (UACC) for minidisk SECADM.191 from READ to NONE.

Known: User SECADM has the SPECIAL attribute. Minidisk SECADM.191 is defined to RACF with a UACC of READ.

Command:
```
RALTER VMMDISK SECADM.191 UACC(NONE)
```

Defaults: None

RDEFINE (Define General Resource Profile)

System environment

This command applies to both z/OS and z/VM systems.

Purpose

Use the RDEFINE command to define to RACF all resources belonging to classes specified in the class descriptor table (CDT). You can also use the RDEFINE command to create entries in the global access checking table and entries in the lists of security categories and security levels.

You cannot, however, use the RDEFINE command to define users, groups, or data sets.

To have changes take effect after defining a generic profile if the class is not RACLISTed by SETROPTS RACLIST, one of the following steps is required:

- The security administrator issues the SETROPTS command:

  ```
  SETROPTS GENERIC(class-name) REFRESH
  ```

  See the SETROPTS command for authorization requirements.
- The user of the resource logs off and logs on again.

To have changes take effect after defining a generic profile if the class is RACLISTed, the security administrator issues the following command:

```
SETROPTS RACLIST(class-name) REFRESH
```

For more information, refer to *z/VM: RACF Security Server Security Administrator's Guide*.

Related Commands

- To create an SFS file profile, use the ADDFILE command as described in “ADDFILE (Add SFS File Profile)” on page 22.
- To create an SFS directory profile, use the ADDDIR command as described in “ADDDIR (Add SFS Directory Profile)” on page 16.
- To create a group profile, use the ADDGROUP command as described in “ADDGROUP (Add Group Profile)” on page 28.
- To create a data set profile, use the ADDSD command as described in “ADDSD (Add Data Set Profile)” on page 33.
- To create a user profile, use the ADDUSER command as described in “ADDUSER (Add User Profile)” on page 45.
- To permit or deny access to a general resource profile, use the PERMIT command as described in “PERMIT (Maintain Resource Access Lists)” on page 202.
- To change a general resource profile, use the RALTER command as described in “RALTER (Alter General Resource Profile)” on page 213.
- To delete a general resource profile, use the RDELETE command as described in “RDELETE (Delete General Resource Profile)” on page 244.

The command adds a profile for the resource to the RACF data base in order to control access to the resource. It also places your user ID on the access list and gives you ALTER authority to the resource.

Authorization Required

To use the RDEFINE command, you must have the SPECIAL attribute or be authorized as follows:

- If you have CLAUTH authority to the GLOBAL resource group within the scope of the same group in which you also have the group-SPECIAL attribute, you can add global resources where the high-level qualifier is the group name or a user ID owned by the group.
- If the resource to be defined is not already defined to RACF as a member of a resource group, you must be authorized to define resources for the specified class. (This authority can be established with the CLAUTH operand on the ADDUSER or ALTUSER command.)
- If the resource to be defined is a discrete name already defined to RACF as a member of a resource group, you can define it as a resource to RACF if you have ALTER authority, or if the resource group profile is within the scope of a group in which you have the group-SPECIAL attribute, or if you are the owner of the resource group profile. If authority conflicts arise because the resource is a member of more than one group and the user's authority in those groups differs, RACF resolves the conflict by using the least restrictive authority (unless modified by the installation).
- To use the ADDMEM operand, you must have ALTER authority to the member resource or be the owner of the member resource, or the member resource must be within the scope of a group in which you have the group-SPECIAL attribute. To add a resource that is not defined to RACF, you must be authorized to define resources in the member class (using the CLAUTH operand on the ADDUSER or ALTUSER command).
- To use the ADDMEM operand if *class-name* is specified as GLOBAL and *profile-name-1* is specified as DATASET, either you must have the SPECIAL attribute, or the member must be within the scope of a group in which you the group-SPECIAL attribute, or the high-level qualifier of the member name must be your user ID.
- If the SETROPTS GENERICOWNER option is in effect, and if a generic profile already exists, *more specific* profiles that protect the same resources can be created only by the following users:
  - The owner of the existing generic profile
  - A user with system-SPECIAL
  - A user with group-SPECIAL if the group owns the profile
  - A user with group-SPECIAL if the owner of the existing profile is in the group
- To assign a security category to a profile, you must have the SPECIAL attribute or have the category in your user profile.
- To assign a security level to a profile, you must have the SPECIAL attribute or, in your own profile, a security level that is equal to or greater than the security level you are defining.
- To define the DLFDATA, SESSION, or SSIGNON segment, you must have the SPECIAL attribute, or your installation must permit you to do so through field level access checking.
- To assign a security label to a profile, you must have the SPECIAL attribute or have READ access to the security label profile. However, the security administrator can limit the ability to assign security labels to only users with the SPECIAL attribute.

Model profiles: To specify a model profile (using, as required, FROM, FCLASS, FGENERIC, and FVOLUME), you must have sufficient authority over the model profile—the “from” profile. RACF makes the following checks until one of the conditions is met:

- You have the SPECIAL attribute
- The “from” profile is within the scope of a group in which you have the group-SPECIAL attribute
- You are the owner of the “from” profile
- If the FCLASS operand is DATASET, the high-level qualifier of the profile name (or the qualifier supplied by the naming conventions routine or a command installation exit) is your user ID.
- If the FCLASS operand is FILE or DIRECTRY or defaults to FILE or DIRECTRY, the userid qualifier of the profile name is your user ID.

For discrete profiles only, the following apply:

- You are on the access list in the "from" profile with ALTER authority. (If you have any lower level of authority, you cannot use the profile as a model.)
- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is in the access list in the "from" profile with ALTER authority. (If any group that RACF checked has any lower level of authority, you cannot use the profile as a model.)
- The universal access authority (UACC) is ALTER.

Syntax

The following operands used with the RDEFINE command apply to z/OS systems only:

- DLFDATA
- FVOLUME
- SESSION(CONVSEC)
- SINGLEDSN
- TVTOC.

The complete syntax of the command is:

```
RDEFINE                 ***class-name***
RDEF                    (***profile-name-1 ...***)
                        [ ADDCATEGORY(category-name ...) ]
                        [ ADDMEM(member ...) ]
                        [ APPLDATA('application-data') ]
                        [ AUDIT( access-attempt [(audit-access-level)] ...) ]
                        [ DATA('installation-defined-data') ]
                        [ FCLASS(profile-name-2-class) ]
                        [ FGENERIC ]
                        [ FROM(profile-name-2) ]
                        [ LEVEL(nn) ]
                        [ NOTIFY[(userid)] ]
                        [ OWNER (userid or group-name) ]
                        [ SECLABEL(seclabel-name) ]
                        [ SECLEVEL(seclevel-name) ]
                        [ SESSION(
                          [ INTERVAL(n) ]
                          [ LOCK ]
                          [ SESSKEY(session-key) ]
                          ) ]
                        [ SSIGNON(
                          [ KEYMASKED(key-value)
                          | KEYENCRYPTED(key-value)]) ]
                        [ TIMEZONE( {E | W} hh[.mm] ) ]
                        [ UACC(access-authority) ]
                        [ WARNING ]
                        [ WHEN( [DAYS(day-info)] [TIME(time-info)] ) ]
```

z/OS Specific Operands:	[DLFDATA([RETAIN(YES | NO)] [JOBNAMES(*jobname-1* ...)])] [FVOLUME(*profile-name-2-serial*)] [SINGLEDSN] [SESSION([CONVSEC(NONE | CONV | PERSISTV | ALREADYV | AVPV))] [TVTOC]

Parameters

class-name
specifies the name of the class to which the resource belongs. The valid class names are those defined in the class descriptor table (CDT). For a list of general resource classes supplied by IBM, see Appendix B, "IBM-Supplied Resource Classes that Apply to z/VM Systems," on page 349.

This operand is required and must be the first operand following RDEFINE.

profile-name-1
specifies the name of the discrete or generic profile you want to add to the specified class. RACF uses the class descriptor table (CDT) to determine if the class is defined to RACF, the syntax of resource names within the class, and whether the resource is a group resource. For more information, see Appendix A, "Resource Profile Naming Considerations," on page 335 and *z/VM: RACF Security Server Security Administrator's Guide*.

This operand is required and must be the second operand following RDEFINE.

On both z/OS and z/VM systems:

- If you specify more than one profile name, you must enclose the list of names in parentheses.
- If you specify *class-name* as GLOBAL, *profile-name-1* must be either DATASET or a valid class name (other than a resource group class) as specified in the CDT. If you specify *class-name* as GLOBAL or SECDATA and also specify ADDMEM or DELMEM, you can specify only one profile name.
- If *class-name* is a resource grouping class, you cannot specify a generic *profile-name-1*.

On z/OS systems only:

- If you specify *class-name* as PROGRAM, you can specify only one profile name, and you must specify the ADDMEM or DELMEM operand.
- If you specify *class-name* as PROGRAM, *profile-name* must be the name of a load module. If you specify the full name of the load module, the profile applies only to that module. If you specify the last character of the name as an asterisk (*), the profile applies to all load modules that match the preceding part of the name, and these load modules must all reside in the same library. For example, IKF* identifies all load module names that begin with IKF. If you specify *profile-name* as an asterisk (*), the profile applies to all load modules that reside in the library you identify on the ADDMEM or DELMEM operand.
- If you are activating field level access checking, you must specify *class-name* as FIELD. To define a profile (*profile-name-1*) in the FIELD class, you must follow the naming conventions described in the section on field level access checking in *z/VM: RACF Security Server Security Administrator's Guide*.

Note:

1. Do not specify a generic character unless SETROPTS GENERIC (or SETROPTS GENCMD) is in effect.

2. RACF processes each resource you specify independently, and all operands you specify apply to each named resource. If an error occurs while it is processing a resource, RACF issues a message and continues processing with the next resource.

ADDCATEGORY(*category-name* ...)
specifies one or more names of installation-defined security categories. The names you specify must be defined as members of the CATEGORY profile in the SECDATA class. (For information on defining security categories, see *z/VM: RACF Security Server Security Administrator's Guide*.)

When the SECDATA class is active and you specify ADDCATEGORY, RACF performs security category checking in addition to its other authorization checking. If a user requests access to a resource, RACF compares the list of security categories in the user's profile with the list of security categories in the resource profile. If RACF finds any security category in the resource profile that is not in the user's profile, RACF denies access to the resource. If the user's profile contains all the required security categories, RACF continues with other authorization checking.

Note: RACF does not perform security category checking for an z/OS started procedure with the privileged attribute, or when the resource you are defining is in the PROGRAM class.

When the SECDATA class is not active, RACF ignores this operand. When the CATEGORY profile does not include a member for a category name, you are prompted to provide a valid one.

ADDMEM(*member* ...)
specifies the member names that RACF is to add to the profile indicated by *profile-name-1*. The meaning of “member” varies, depending on the class.

You can use the ADDMEM operand to perform tasks such as defining security categories and security levels, entries in the global access checking table, and entries for program control as described in the following sections.

In addition to the authority needed to issue the RDEFINE command, you need one of the following authorities to add members using the RDEFINE command:

1. For classes other than PROGRAM, SECDATA, GLOBAL, RACFVARS, NODES, and VMXEVENT, if the member resources are already RACF-protected by a member class profile or as a member of a profile in the same grouping class, one of the following must be true:
   - You have ALTER access authority to the member.
   - You are the owner of the member resource.
   - The member resource is within the scope of a group in which you have the group-SPECIAL attribute.
   - You have the SPECIAL attribute.
2. For classes other than PROGRAM, SECDATA, GLOBAL, RACFVARS, NODES, and VMXEVENT, if the member resources are not RACF-protected (that is, there is no profile defined for that member), one of the following must be true:
   - You have CLAUTH authority to define resources in the member resource class.
   - You have the SPECIAL attribute.
3. To add a member to a profile in the RACFVARS or NODES class, one of the following must be true:
   - You have CLAUTH authority to define resources in the specified class (for example, RACFVARS or NODES).
   - You have the SPECIAL attribute.
   - You are the owner of the profile indicated by *profile-name-1*.
   - You have ALTER access authority to the profile indicated by *profile-name-1*.
4. To add a member to a profile in the PROGRAM or SECDATA class, one of the following must be true:

- You have CLAUTH authority to define resources in the specified class (for example, PROGRAM or SECDATA).
- You have the SPECIAL attribute.

5. To add a member to a profile in the GLOBAL class (other than the GLOBAL FILE, GLOBAL DIRECTRY, or GLOBAL DATASET profile) where the syntax is:

   ```
   RDEF GLOBAL class-name ADDMEM(resource-name/access-level)
   ```

   one of the following must be true:

   - If the profile *resource-name* is already RACF-protected by a profile in class *class-name*:
     - You have ALTER access authority to the profile *resource-name* in class *class-name*.
     - You are the OWNER of the profile *resource-name*.
     - The profile *resource-name* in class *class-name* is within the scope of a group in which you have the group-SPECIAL attribute.
     - You have the SPECIAL attribute.
   - If the profile *resource-name* is not already RACF-protected (that is, there is no profile defined for that member in class *class-name*):
     - You have CLAUTH authority to define resources in the class *class-name*.
     - You have the SPECIAL attribute.

6. To add a member to the GLOBAL DATASET profile, one of the following must be true:
   - You are the owner of the DATASET profile in the GLOBAL class.
   - The member is within the scope of a group in which you have the group-SPECIAL attribute, or the high-level qualifier of the member name is your user ID.
   - You have the SPECIAL attribute.
7. To add a member to the GLOBAL DIRECTRY or GLOBAL FILE profile, you must have the SPECIAL attribute.
8. To add a member to a profile in the VMXEVENT class, the following rules apply:
   - To set the control options (add a member specifying /CTL or /NOCTL), you must have the SPECIAL attribute.
   - To set the audit options (add a member specifying /AUDIT), you must have the AUDITOR attribute.

RACF ignores the ADDMEM operand if the class name you specify is not a resource grouping class, GLOBAL, SECDATA, NODES, or PROGRAM.

Specifying Member on the ADDMEM Operand

Following are discussions on how to specify *member* depending on the class of the profile.

- *When a Resource Grouping Class is the class-name*

  Resource Grouping Class: If the class-name is a resource grouping class, the members you specify through the ADDMEM operand will protect the resources in the related member class.

  If generic profile checking is active for the related member class, you can include a generic character (*, **, &, or % only) in the member to protect multiple resources.

  For more information on resource grouping classes and their related member classes, see *z/VM: RACF Security Server Security Administrator's Guide*.

- *When GLOBAL is the class-name*

  Global Access Checking: You can define an entry in the global access checking table by issuing the RDEFINE command with the following operands:

  – GLOBAL as the class-name

- The appropriate resource class name as profile-name
- ADDMEM with the name of the entry you are defining (as *member*). (If the name you specify as *member* contains a generic character (*, ** or %), generic profile checking (SETROPTS command with the GENERIC operand) must be active for the resource class you specify as *profile-name*.)
- The access level you are assigning to the entry (member) using the following format:

```
member   [ / {ALTER  } ]
         {CONTROL}
         {NONE   }
         {READ   }
         {UPDATE }
```

The format of this command is as follows:

```
RDEFINE GLOBAL profile-name ADDMEM(member/access-level)
```

Each entry you define controls global access checking for the resources matching that entry name.

Attention:
Because RACF performs global access checking before security classification processing, global access checking might allow access to a resource you are protecting with a security category, security level, or both. To avoid a security exposure to a sensitive resource, do not define an entry in the global access checking table for a resource you are protecting with security classification processing.

Note that FRACHECK processing does not include global access checking.

When you define an entry in the global access checking table, specify *member* on the ADDMEM operand as described in the following sections. When you define an entry in the global access checking table for a data set, enclose the entry name in quotes if you do not want your TSO prefix (which might be your user ID) used as the high-level qualifier of the entry name.

For example, assume that your user ID is SMITH. If you issue the following command:

```
RDEFINE GLOBAL DATASET ADDMEM('SMITH.ABC'/READ)
```

you define the entry SMITH.ABC in the global access table.

If you do not enclose the entry name in quotes, your TSO prefix will be used as the high-level qualifier of the entry name. For example, if you issue the following command:

```
RDEFINE GLOBAL DATASET ADDMEM(ABC/READ)
```

you define the entry SMITH.ABC in the global access table.

If the entry name you specify contains * as the high-level qualifier and you do not enclose the name in quotes, RACF creates the entry exactly as you specify it (your TSO prefix will **not** be used as the high-level qualifier of the entry name). For example, if you issue the following command:

```
RDEFINE GLOBAL DATASET ADDMEM(*.ABC/READ)
```

you define the entry *.ABC in the global access table. If you enclose *.ABC in quotes, you define the same entry (*.ABC) in the global access table.

Global Access Checking for General Resources: To define an entry in the global access checking table for a general resource, specify any valid class name in the IBM-supplied or installation-defined class descriptor table (CDT) as a profile name. (For a list of general resource classes supplied by IBM, see Appendix B, “IBM-Supplied Resource Classes that Apply to z/VM

Systems," on page 349.) The member name you specify with the ADDMEM operand can contain one or more generic characters (% or *) that you can use as follows:

- Specify % to match any single character in a resource name
- Specify * as the last character of an entry name to match zero or more characters until the end of a resource name or, by itself, to match an entire resource name.

Global Access Checking for the FILE and DIRECTRY Classes: To define an entry in the global access checking table for an SFS file or directory, you must use the RACF format rather than the SFS format. For the format of these profile names, see "Profile Names for SFS Files and Directories" on page 342.

If your file name is `FN FT FP:USER.A`, use `FP.USER.A.FN.FT`.

If your directory name is `FP:USER.A.B`, use `FP.USER.A.B`.

- *When SECDATA is the class name*

  Security Classification of Users and Data: To define a security category or security level for your installation, specify *class-name* as SECDATA and *profile-name* as one of the following:

  - CATEGORY when defining a security category
  - SECLEVEL when defining a security level.

  If you specify SECDATA CATEGORY, the ADDMEM operand specifies the name of an installation-defined category of users.

  For example, to define three categories of users named CODE, TEST, and DOC, enter:

```
RDEFINE SECDATA CATEGORY ADDMEM(CODE TEST DOC)
```

  The security category name can be from 1 through 44 characters in length and must not contain a blank, comma, semicolon, right parenthesis, or, on z/VM systems, your line editing characters unless you turn off line editing.

  If you specify SECDATA SECLEVEL, the ADDMEM operand specifies both the name of an installation-defined security level and the number you assign to that level, in the form:

```
seclevel-name/seclevel-number
```

  You must separate the two items by a slash (/). The *seclevel-name* can be from 1 through 44 characters in length, and must not contain a blank, comma, semicolon, right parenthesis, or, on z/VM systems, your line editing characters unless you turn off line editing. The *seclevel-number* can be any number from 1 through 254. The higher the number, the higher the security level. For example, to define three security levels, where CONFIDENTIAL is the most restrictive, enter:

```
RDEFINE SECDATA SECLEVEL +
  ADDMEM(GENERAL/10 EXPERIMENTAL/75 CONFIDENTIAL/150)
```

  Because RACF keeps track of security levels by number, replacing an existing security level name does not affect the protection that the security level number provides. If you had defined the security levels shown in the preceding example and then replaced GENERAL/10 with INTERNAL/10, a listing of a user or resource profile that included security level 10 would show the new name. Because the security level number is the same, there is no need to change any resource or user profiles.

  When you actually change an existing CATEGORY profile or SECLEVEL profile, however, RACF issues a warning message to remind you that the change is not reflected in existing resource or user profiles. In this case, you can use the SEARCH command to locate the profiles you must modify.

- *When NODES is the class-name*

  Translation of User IDs, Group ID, or Security Labels on Inbound Jobs or SYSOUT:

If the class-name is NODES, you can specify how user IDs, group IDs, and security labels are translated. The translation depends on the second and third qualifiers of the profile name, as follows:

If the Second Qualifier Is:	The ADDMEM Value Specifies:
USERJ	The user ID to be used on this system for the inbound jobs to which the profile applies
USERS	The user ID to be used on this system for the inbound SYSOUT to which the profile applies
GROUPJ	The group ID to be used on this system for the inbound jobs to which the profile applies
GROUPS	The group ID to be used on this system for the inbound SYSOUT to which the profile applies
SECLJ	The security label to be used on this system for the inbound jobs to which the profile applies
SECLS	The security label to be used on this system for the inbound SYSOUT to which the profile applies

For information on setting up NODES profiles, see *z/VM: RACF Security Server Security Administrator's Guide*.

- *When VMXEVENT is the class-name*

  Auditing or Controlling z/VM Events: If the *class-name* is VMXEVENT *member* must be the RACF name for the z/VM event, followed by an option that describes the action RACF is to take when the z/VM event occurs. Specify the member entry in the following format:

  ```
  event-name/option
  ```

  event-name
  specifies the RACF event name of the z/VM event to be audited or controlled.

  option
  specifies one of the following:

  - **AUDIT** z/VM calls RACF to audit occurrences of this event. This option can be used only by a user with the system AUDITOR attribute.
  - **CTL** z/VM calls RACF to authorize use of this event. This option can be used only by a user with the system SPECIAL attribute.
  - **NOCTL** z/VM stops calling RACF to authorize use of this event. This option can be used only by a user with the system SPECIAL attribute.

  For a complete description of how to audit selected z/VM events, refer to the *z/VM: RACF Security Server Security Administrator's Guide*. For information on how to control access to selected z/VM Events, see *z/VM: RACF Security Server Security Administrator's Guide*.

- *When PROGRAM is the class-name*

  Program Control on z/OS: If you specify *class-name* as PROGRAM, *profile-name* must identify one or more controlled programs, and *member* describes the entry for each in the in-storage profile table of controlled programs. You specify the member entry in the following format: `library-name/volser/PADCHK` or `NOPADCHK`

  library-name
  specifies the name of the library in which the controlled programs reside. If *profile-name* is an asterisk, RACF treats all load modules in the specified library as controlled programs.

volser
specifies the serial number of the volume on which the library resides. You can use six asterisks within single quotation marks to specify the current SYSRES volume: `library-name/'******'/PADCHK` or `NOPADCHK`

PADCHK | NOPADCHK
specifies that RACF is to make (PADCHK) or not to make (NOPADCHK) the checks for program-accessed data sets when a user is executing the controlled programs. If you specify PADCHK, RACF verifies that (1) the conditional access list in the profile for a program-accessed data set allows the access and (2) no task in the user's address space has previously loaded a non-controlled program.

If you specify NOPADCHK, RACF does not perform this extra checking to verify that a non-controlled program cannot access a program-accessed data set. NOPADCHK allows you, for example, to define entire libraries of modules (such as ISPF) as controlled programs without then having to grant each of these modules access to many program-accessed data sets. Examples 3 and 4 on page "Examples" on page 241 show two ways to define controlled programs. If you need more information on program control, see *z/VM: RACF Security Server Security Administrator's Guide*.

APPLDATA('*application-data*')
This parameter specifies a text string that will be associated with each of the named resources. The text string can contain a maximum of 255 characters and must be enclosed in single quotation marks. It can also contain double-byte character set (DBCS) data.

For the TIMS and GIMS class, to force the user to reenter his password whenever the transaction or transactions listed in the *profile-name-1* or ADDMEM operands are used, specify *application-data* as `REVERIFY`.

This information, if present, can be displayed with the RLIST command and will be included in the resident profile generated by RACLIST.

AUDIT(*access-attempts*[(*audit-access-level*)])

access-attempts
specifies which access attempts you want to log on the SMF data set for z/OS or the SMF data file for z/VM. The following options are available:

ALL
indicates that you want to log both authorized accesses and detected unauthorized access attempts.

FAILURES
indicates that you want to log detected unauthorized access attempts.

NONE
indicates that you do not want any logging to be done.

SUCCESS
indicates that you want to log authorized accesses to the resource.

audit-access-level
specifies which access levels you want to log on the SMF data set for z/OS or the SMF data file for z/VM. The levels you can specify are:

ALTER
logs ALTER access-level attempts only.

CONTROL
logs access attempts at the CONTROL and ALTER levels.

READ
logs access attempts at any level. This is the default value if no access level is specified.

UPDATE
logs access attempts at the UPDATE, CONTROL, and ALTER levels.

FAILURES(READ) is the default value if the AUDIT operand is omitted from the command.

You cannot audit access attempts for the EXECUTE level.

DATA('*installation-defined-data*')
specifies up to 255 characters of installation-defined data to be stored in the profile for the resource. The data must be enclosed in single quotation marks. It can also contain double-byte character set (DBCS) data.

This information is listed by the RLIST command. It is also available to RACF postprocessing installation exit routines for RACHECK (for resources belonging to classes defined in the class descriptor table) or RACINIT (for APPL and TERMINAL) SVCs.

DLFDATA
Note: *This operand applies to z/OS systems only.*

for profiles in the DLFCLASS, specifies information used in the control of DLF objects

RETAIN(YES | NO)
specifies whether the DLF object can be retained after use

JOBNAMES(*jobname-1 ....*)
specifies the list of objects which can access the DLF objects protected by this profile.

You can specify any job name valid on your system. You can also specify generic job names with an asterisk (*****) as the last character of the job name. For example, JOBNAMES(ABC) will allow only job ABC to access the DLF objects protected by the profile. JOBNAMES(ABC*) will allow any job whose name begins with ABC (such as ABC, ABC1, or ABCDEF and so forth) to access the DLF objects.

Note: If DLFDATA is not specified, or is specified without the RETAIN suboperand, RETAIN(NO) is defaulted.

FCLASS(*profile-name-2-class*)
specifies the name of the class to which *profile-name-2* belongs. The valid class names are DATASET or those classes defined in the class descriptor table (CDT). For a list of general resource classes defined in the IBM-supplied CDT, see Appendix B, “IBM-Supplied Resource Classes that Apply to z/VM Systems,” on page 349.

If you omit this operand, RACF assumes that *profile-name-2* belongs to the same class as *profile-name-1*. This operand is valid only when you also specify the FROM operand; otherwise, RACF ignores it.

FGENERIC
specifies that RACF is to treat *profile-name-2* as a generic name, even if it is fully qualified (meaning that it does not contain any generic characters). This operand is needed only if *profile-name-2* is a DATASET profile.

FROM(*profile-name-2*)
specifies the name of an existing discrete or generic profile that RACF is to use as a model for the new profile. The model profile name you specify on the FROM operand overrides any model name specified in your user or group profile. If you specify FROM and omit FCLASS, RACF assumes that *profile-name-2* is the name of a profile in the same class as *profile-name-1*.

To specify FROM, you must have sufficient authority to both *profile-name-1* and *profile-name-2,* as described under “RACF Requirements.”

Possible Changes to Copied Profiles When Modeling Occurs

When a profile is copied during profile modeling, the new profile may differ from the model in the following ways:

- RACF places the user on the access list with ALTER access authority or, if the user is already on the access list, changes the user's access authority to ALTER.
- If the model profile contains members (specified with the ADDMEM operand), the members are not copied into the new profile.

- If the SETROPTS MLS option is in effect, the security label (if specified in the model profile) is not copied. Instead, the user's current security label is used.

  EXCEPTION: When SETROPTS MLS and MLSTABLE are both in effect and the user has the SPECIAL attribute, the security label specified in the model profile is copied to the new profile.
- For TAPEVOL profiles, TVTOC information is not copied to the new profile.
- Information in the non-RACF segments (for example, the SESSION or DLFDATA segment) is not copied.

For information about automatic profile modeling, refer to *z/VM: RACF Security Server Security Administrator's Guide*.

FVOLUME(*volume-serial*)
Note: *This operand applies to z/OS systems only.*

FVOLUME specifies the volume RACF is to use to locate the model profile (profile-name-2).

If you specify FVOLUME and RACF does not find *profile-name-2* associated with that volume, the command fails. If you omit this operand and *profile-name-2* appears more than once in the RACF data set, the command fails.

FVOLUME is valid only when FCLASS either specifies or defaults to DATASET and when *profile-name-2* specifies a discrete profile. Otherwise, RACF ignores FVOLUME.

LEVEL(*nn*)
specifies a level indicator, where *nn* is an integer between 0 and 99. The default is 0.

Your installation assigns the meaning of the value. It is available to RACF postprocessing installation exit routines for RACHECK SVCs (for resources belonging to classes defined in the class descriptor table) or RACINIT SVCs (for APPL and TERMINAL). It is included on all records that log resource accesses and is listed by the RLIST command.

NOTIFY[(*userid*)]
specifies the user ID of a user to be notified whenever RACF uses this profile to deny access to a resource. If you specify NOTIFY without specifying a user ID, RACF takes your user ID as the default; you will be notified whenever the profile denies access to a resource.

A user who is to receive NOTIFY messages should log on frequently to take action in response to the unauthorized access attempt described in each message. RACF sends NOTIFY messages as follows:

- On z/OS, RACF sends NOTIFY messages to the SYS1.BRODCAST data set.
- On z/VM, RACF sends NOTIFY messages to the specified user ID. (Note that you should not specify the user ID of a virtual machine that always runs disconnected.) If the user ID is logged on, the message immediately appears on the user's screen. If the user ID is not logged on or is disconnected, RACF sends the message to the user in a reader file. The name of this reader file will be the user ID specified on the NOTIFY keyword and the type will be NOTIFY.

When the resource profile also includes WARNING, RACF might have granted access to the resource to the user identified in the message. RACF does **not** notify a user when it denies access to a resource if the resource is in a class for which your installation has built in-storage profiles using the RACLIST macro. Profiles built using the RACLIST macro are made resident by certain resource managers, such as IMS and CICS, so that they can be used by the FRACHECK facility for authorization checking. FRACHECK does not issue NOTIFY messages. However, it provides return and reason codes to its caller so they can ensure appropriate auditing.

OWNER(*userid* or *group-name*)
specifies a RACF-defined user or group to be assigned as the owner of the resource you are defining. If you omit this operand, you are defined as the owner. The user specified as the owner does not automatically have access to the resource. Use the PERMIT command to add the owner to the access list as desired.

SECLABEL(*seclabel-name*)
specifies the user's resource's default security label, where *seclabel-name* is an installation-defined security label name that represents an association between a particular security level and a set of zero or more categories.

A security label corresponds to a particular security level (such as CONFIDENTIAL) with a set of zero or more security categories (such as PAYROLL or PERSONNEL).

For a list of security labels that you are authorized to use, enter:

```
SEARCH CLASS(SECLABEL)
```

RACF stores the name of the security label you specify in the resource profile if you are authorized to use that SECLABEL.

If you are not authorized to the SECLABEL or if the name you had specified is not defined as a SECLABEL profile in the SECLABEL class, the resource profile is not created.

SECLEVEL(*seclevel-name*)
specifies the name of an installation-defined security level. The name corresponds to the number that is the minimum security level that a user must have to access the resource. The *seclevel-name* must be a member of the SECLEVEL profile in the SECDATA class.

When you specify SECLEVEL and the SECDATA class is active, RACF adds security level checking to its other authorization checking. If global access checking grants access, RACF compares the security level allowed in the user profile with the security level required in the resource profile. If the security level in the user profile is less than the security level in the resource profile, RACF denies the access. If the security level in the user profile is equal to or greater than the security level in the resource profile, RACF continues with other authorization checking. The SECLEVEL operand is required for the SECLABEL class.

Note: RACF does not perform security level checking for a started procedure with the privileged attribute, or when the resource you are defining is in the PROGRAM class.

If the SECDATA class is not active, RACF stores the name you specify in the resource profile. When the SECDATA class is activated and the name you specified is defined as a SECLEVEL profile, RACF can perform security level access checking for the resource profile. If the name you specify is not defined as a SECLEVEL profile, you are prompted to provide a valid SECLEVEL name.

SESSION
is only valid for the APPCLU resource class. It specifies that when changing an APPCLU class profile, the following suboperands add, change, or delete SESSION segment field values. The SESSION segment is used to control the establishment of sessions between logical units under LU6.2.

CONVSEC
Note: *This operand applies to z/OS systems only.*

specifies the level or levels of security checking performed when conversations are established with the LU protected by this profile.

Note: In general, you should select one of ALREADYV, AVPV, CONV, NONE or PERSISTV for each APPCLU profile.

ALREADYV
APPC/MVS™ RACF does *not* verify the user ID and password for any inbound allocate requests. If you specify ALREADYV, you assume that user IDs and passwords have already been verified by the partner LU. You must specify this only if the partner LU is trustworthy.

AVPV
The user ID/password is already verified and persistent verification is requested.

CONV
APPC/MVS issues a RACINIT request to verify the user ID and password for all inbound allocate requests.

NONE
All inbound allocate requests pass without RACF checking for a valid user ID. No RACINIT request is issued.

PERSISTV
Specifies persistent verification.

INTERVAL(*n*)
sets the maximum number of days the session key is valid. The variable *n* is in the range of 1 to 32767. If the key interval is longer than the installation maximum (set with SETROPTS SESSIONINTERVAL), then the profile will not be created.

If the key interval is not specified and there is a SETROPTS SESSIONINTERVAL value, the profile is created with that value. If there is no SETROPTS SESSIONINTERVAL value, there is no limit to the number of days the session key is valid.

LOCK
mark the profile as locked. This prevents all session establishment from succeeding.

SESSKEY(*session-key*)
change the key for this profile. The variable *session-key* can be expressed in two ways:

- X'y'—where y is a 1- to 16-digit hexadecimal number
- z or 'z'—where z is a one- to eight-character string

If the entire 16 digits or eight characters are not used, the field is padded to the right with binary zeros.

SINGLEDSN
Note: *This operand applies to z/OS systems only.*

SINGLEDSN specifies that the tape volume can contain only one data set. SINGLEDSN is valid only for a TAPEVOL profile. If the volume already contains more than one data set, RACF issues a message and ignores the operand.

SSIGNON(KEYMASKED(*key-value*)|(KEYENCRYPTED(*key-value*))
defines the secured signon application key and indicates the method you want to use to protect the key value within the RACF database on the host. When defining the profile, you can either mask or encrypt the key. The *key-value* represents a 64-bit (8-byte) key that must be represented as 16 hexadecimal characters. The valid characters are 0 through 9 and A through F.

Note:

1. As with RACF passwords, the database unload facility does not unload secured signon application keys.
2. The RLIST command does not list the value of the secured signon application keys. Therefore, when you define the keys, you should note the value and keep it in a secure place.
3. These operands can be specified only via the RACF commands; they are not available in the ISPF panels.

KEYMASKED(*key-value*)
indicates that you want to mask the key value using the masking algorithm.

Note:

1. You can specify this operand only once for each application key.
2. If you mask a key, you *cannot* encrypt it. These are mutually exclusive.

You can use the RLIST command to ensure that the key is protected.

KEYENCRYPTED(*key-value*)
indicates that you want to encrypt the key value.

Note:

1. You can specify this operand only once for each application key.

2. If you encrypt a key, you *cannot* mask it. These are mutually exclusive.
3. A cryptographic product must be installed and active on the system.

You can use the RLIST command to verify that the key is protected.

TIMEZONE({E | W} *hh*[.*mm*])
specifies the time zone in which a terminal resides. TIMEZONE is valid only for resources in the TERMINAL class; RACF ignores it for all other resources.

Specify TIMEZONE only when the terminal is not in the same time zone as the processor on which RACF is running and you are also specifying WHEN to limit access to the terminal to specific time periods. In this situation, TIMEZONE provides the information RACF needs to calculate the time values correctly. If you identify more than one terminal in the *profile-name-1* operand, all the terminals must be in the same time zone.

On TIMEZONE, you specify whether the terminal is east (E) or west (W) of the system and by how many hours (hh) and, optionally, minutes (mm) that the terminal time zone is different from the processor time zone. Valid hour values are 0 through 11, and valid minute values are 00 through 59.

For example, if the processor is in New York and the terminal is in Los Angeles, specify TIMEZONE(W 3). If the processor is in Houston and the terminal is in New York, specify TIMEZONE(E 1).

If you change the local time on the processor (to accommodate daylight savings time, for instance), RACF adjusts its time calculations accordingly. If, however, the processor time zone and the terminal time zone do not change in the same way, you must adjust the terminal time zones yourself, as described earlier for the WHEN(TIME) operand.

TVTOC
Note: *This operand applies to z/OS systems only.*

specifies, for a TAPEVOL profile, that RACF is to create a TVTOC in the TAPEVOL profile when a user creates the first output data set on the volume. The RDEFINE command creates a non-automatic TAPEVOL profile; RACF creates and maintains the TVTOC for datasets residing on tape.

Specifying TVTOC also affects the access list for the TAPEVOL profile:

1. When RACF processes the RDEFINE command with the TVTOC operand, it places the user ID of the command issuer (perhaps the tape librarian) in the access list with ALTER authority.
2. When the first output data set is created on the volume, RACF adds the user ID associated with the job or task to the access list with ALTER authority.

See *z/VM: RACF Security Server Security Administrator's Guide* for further information.

The TVTOC operand is valid only for a discrete profile in the TAPEVOL class.

UACC(*access-authority*)
specifies the universal access authority to be associated with this resource. The universal access authorities are ALTER, CONTROL, UPDATE, READ, EXECUTE (for controlled programs only), and NONE. If UACC is not specified, RACF uses the value in the ACEE or the class descriptor table. If UACC is specified without *access-authority*, RACF uses the value in the current connect group. On z/OS, for tape volumes and DASD volumes, RACF treats CONTROL authority as UPDATE authority. On both z/OS and z/VM for all other resources listed in the class descriptor table and for applications, RACF treats CONTROL and UPDATE authority as READ authority.

WARNING
specifies that, even if access authority is insufficient, RACF is to issue a warning message and allow access to the resource. However, z/VM CP initiated requests (for example, LINK commands) are either deferred to CP or rejected, depending on the configuration of the SYSSEC macro. For information about the SYSSEC macro, see *z/VM: RACF Security Server Macros and Interfaces*. RACF also records the access attempt in the SMF record if logging is specified in the profile. RACF does *not* issue a warning message for a resource:

- When the resource is in the PROGRAM class
- When the resource is in the NODES class

- When the resource is in a class for which your installation has built in-storage profiles using the RACLIST macro. Profiles built using the RACLIST macro are made resident by certain resource managers like IMS and CICS so that they can be used by the FRACHECK facility for authorization checking. FRACHECK does not issue warning messages.

WHEN([DAYS(*day-info*)][TIME(*time-info*)])
specifies, for a resource in the TERMINAL class, the days of the week or the hours in the day when a user can access the system from the terminal. The day-of-week and time restrictions apply only when a user logs on to the system; that is, RACF does not force the user off the system if the end-time occurs while the user is logged on.

If you omit the WHEN operand, a user can access the system from the terminal at any time. If you specify the WHEN operand, you can restrict the use of the terminal to certain days of the week or to a certain time period on each day. Or, you can restrict access to both certain days of the week and to a certain time period within each day.

DAYS(*day-info*)
To allow use of the terminal only on certain days, specify DAYS(*day-info*), where *day-info* can be any one of the following:

ANYDAY
RACF allows use of the terminal on any day. If you omit DAYS, ANYDAY is the default.

WEEKDAYS
RACF allows use of the terminal only on weekdays (Monday through Friday).

day...
RACF allows use of the terminal only on the days specified, where day can be MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, or SUNDAY. You can specify the days in any order.

TIME(*time-info*)
To allow use of the terminal only during a certain time period of each day, specify TIME(*time-info*), where *time-info* can be any one of the following:

ANYTIME
RACF allows use of the terminal at any time. If you omit TIME, ANYTIME is the default.

start-time*:*end-time
RACF allows use of the terminal only during the specified time period. The format of both start-time and end-time is *hhmm*, where *hh* is the hour in 24-hour notation (00 through 24) and *mm* is the minutes (00 through 59) within the range 0001 - 2400. Note that 2400 indicates 12:00 a.m. (midnight).

If *start-time* is greater than *end-time*, the interval spans midnight and extends into the following day.

Specifying *start-time* and *end-time* is straightforward when the processor on which RACF is running and the terminal are in the same time zone; you specify the time values in local time.

If, however, the terminal is in a different time zone from the processor and you want to restrict access to certain time periods, you have two choices. You can specify the TIMEZONE operand to allow RACF to calculate the time and day values correctly. Otherwise, you can adjust the time values yourself, by translating the *start-time* and *end-time* for the terminal to the equivalent local time for the processor.

For example, assume that the processor is in New York and the terminal is in Los Angeles, and you want to allow access to the terminal from 8:00 A.M. to 5:00 P.M. in Los Angeles. In this situation, you would specify TIME(1100:2000). If the processor is in Houston and the terminal is in New York, you would specify TIME(0900:1800).

If you omit DAYS and specify TIME, the time restriction applies to all seven days of the week. If you specify both DAYS and TIME, RACF allows use of the terminal only during the specified time period and only on the specified days.

Examples

Example 1

Operation: User TBK20 wants to define resource GIMS600 in class GIMS which is a resource group class. He also wants to define TIMS200, TIMS111, TIMS300, and TIMS333 as members of the resource group (GIMS600).

Known: User TBK20 has the CLAUTH attribute for the GIMS and TIMS classes. GIMS is a resource group class, and TIMS is its associated resource member class. TIMS200 and TIMS111 are members of another resource group. The user has ALTER authority to the other resource group.

Command:
```
RDEFINE GIMS GIMS600 ADDMEM(TIMS200 TIMS111
TIMS300 TIMS333)
```

Defaults: OWNER (TBK20) LEVEL(0) AUDIT(FAILURES(READ)) UACC(NONE)

Example 2

Operation: User ADM1 wants to define a generic profile for all resources starting with a “T” belonging to the TIMS class, and to require that users must reenter their passwords whenever they enter any IMS transaction starting with a T.

Known: User ADM1 has the SPECIAL attribute.

Command:
```
RDEFINE TIMS T* APPL('REVERIFY')
```

Defaults: UACC(NONE) OWNER(ADM1) LEVEL(0) AUDIT(FAILURES(READ))

Example 3

Operation: User ADM1 wants to define AMASPZAP as a controlled program with program-accessed data set checking.

Known: User ADM1 has the SPECIAL attribute. AMASPZAP resides in SYS1.LINKLIB on the SYSRES volume. RACF program control is active.

Command:
```
RDEFINE PROGRAM AMASPZAP ADDMEM('SYS1.LINKLIB'/
SYSRES/PADCHK)
```

Defaults: UACC(NONE) OWNER(ADM1) LEVEL(0) AUDIT(FAILURES(READ))

Example 4

Operation: User ADM1 wants to define all load modules that start with IKF as controlled programs that do not require program-accessed data set checking.

Known: User ADM1 has the SPECIAL attribute. All load modules whose names begin with IKF reside in SYS1.COBLIB on the SYSRES volume.

Command:
```
RDEFINE PROGRAM IKF* ADDMEM('SYS1.COBLIB'/
SYSRES/NOPADCHK)
```

Defaults: UACC(NONE) OWNER(ADM1) LEVEL(0) AUDIT(FAILURES(READ))

Example 5

Operation: User JPQ12 wants to define a tape volume labeled DP0123 and allow it to hold a TVTOC. The tape volume will be assigned a UACC of NONE.

Known: User JPQ12 has the SPECIAL attribute.

Command:
```
RDEFINE TAPEVOL DP0123 TVTOC UACC(NONE)
```

Defaults: OWNER (JPQ12) LEVEL(0) AUDIT(FAILURES(READ))

Example 6

Operation: The security administrator wants to define a profile for TSO in the PTKTDATA class. The security administrator wants to direct the command to run under the authority of user OJC11 at node NYTSO.

Known: SIVLE1 is the user ID of the security administrator.

OJC11 has the SPECIAL attribute on node NYTSO.

The profile name is TSOR001.

The *key-value* is e001193519561977 and is to be masked. The security administrator wants to issue the command as a RACF TSO command.

Command:
```
RDEFINE PTKTDATA TSOR001
SSIGNON(KEYMASKED(e001193519561977))
AT(NYTSO.OJC11)
```

Defaults: UACC(NONE)

RDEFINE Examples for z/VM:

Example 7

Operation: User VMADM1 wants to define a z/VM minidisk USERA.191 with a discrete RACF profile. USERA will own the minidisk.

Known: User VMADM1 has the SPECIAL attribute.

Command:
```
RDEFINE VMMDISK USERA.191 UACC(NONE)
OWNER(USERA)
```

Defaults: LEVEL(0) AUDIT(FAILURES(READ))

Example 8

Operation: User VMADM1 wants to define a z/VM minidisk USERA.192 with a discrete RACF profile for USERA. Minidisk USERA.192 will use the same access list created for minidisk USERA.191.

Known: User VMADM1 has the SPECIAL attribute. USERA has created an access list for minidisk USERA.191.

Command:
```
RDEFINE VMMDISK USERA.192 UACC(NONE)
OWNER(USERA) FROM(USERA.191)
```

Defaults: LEVEL(0) AUDIT(FAILURES(READ)) FCLASS(VMMDISK)

Example 9

Operation User VMADM1 wants to define the reader for the RSCS virtual machine so all users can access it.

Known User VMADM1 has the SPECIAL attribute.

Command
```
RDEFINE VMRDR RSCS UACC(UPDATE)
```

Defaults OWNER(VMADM1) LEVEL(0) AUDIT(FAILURES(READ))

RDELETE (Delete General Resource Profile)

System environment

Purpose

Use the RDELETE command to delete RACF resources belonging to classes specified in the class descriptor table.

This command removes the profile for the resource from the RACF database.

To have changes take effect after deleting a generic profile if the class is not RACLISTed by SETROPTS RACLIST, one of the following steps is required:

- The security administrator issues the SETROPTS command:

  ```
  SETROPTS GENERIC(class-name) REFRESH
  ```

  See the SETROPTS command for authorization requirements.
- The user of the resource logs off and logs on again.

To have changes take effect after deleting a generic profile if the class is RACLISTed, the security administrator issues the following command:

```
SETROPTS RACLIST(class-name) REFRESH
```

For more information, refer to *z/VM: RACF Security Server Security Administrator's Guide*.

Related Commands

- To delete a user profile, use the DELUSER command as described in "DELUSER (Delete User Profile)" on page 143.
- To delete a group profile, use the DELGROUP command as described in "DELGROUP (Delete Group Profile)" on page 141.

Authorization Required

To remove RACF protection from a resource in a class specified in the class descriptor table, you must have sufficient authority over the resource, so that one of the following conditions is met:

- You have the SPECIAL attribute
- The resource profile is within the scope of a group in which you have the group-SPECIAL attribute
- You are the owner of the resource

For discrete profiles in classes other than VMMDISK:

- You are on the access list for the resource and you have ALTER authority.
- Your current connect group is on the access list and has ALTER authority.
- The universal access authority for the resource is ALTER.

Syntax

The complete syntax of the RDELETE command is:

RDELETE RDEL	***class-name*** (***profile-name ...***)

Parameters

class-name
specifies the name of the class to which the resource belongs. Valid class names are those specified in the class descriptor table (CDT). For a list of general resource classes defined in the IBM-supplied CDT, see Appendix B, "IBM-Supplied Resource Classes that Apply to z/VM Systems," on page 349.

This operand is required and must be the first operand following RDELETE.

(*profile-name...*)
specifies the name of the existing discrete or generic profile RACF is to delete from the specified class. RACF deletes the profile for any resource you name by deleting it from the RACF database. RACF uses the class descriptor table (CDT) to determine if the class is defined to RACF, the syntax of resource names within the class, and whether the resource is a group.

This operand is required and must be the second operand following RDELETE.

If you specify more than one value for *profile-name*, you must enclose the list of names in parentheses.

If you specify *class-name* as a resource grouping class, you cannot specify a generic profile.

Note: RACF processes each resource you specify independently. If an error occurs while it is processing a resource, RACF issues a message and continues processing with the next resource.

Examples

Example 1

Operation	User ADM2 wants to remove RACF protection from the terminals protected by the generic profile TERM*.
Known	User ADM2 has the SPECIAL attribute.
Command	`RDELETE TERMINAL TERM*`
Defaults	None

Example 2

Operation	User VMADM1 wants to remove RACF protection from z/VM minidisk USERC.191.
Known	User VMADM1 has the SPECIAL attribute.
Command	`RDELETE VMMDISK USERC.191`
Defaults	None

REMOVE (Remove User from Group)

System environment

This command applies to both z/OS and z/VM systems.

Purpose

On both z/OS and z/VM, you can use the REMOVE command to remove a user from a group. In addition, on z/OS, you can use the REMOVE command to assign a new owner to any group data set profiles the user owns on behalf of that group.

Related Commands

- To add a group profile, use the ADDGROUP command as described in "ADDGROUP (Add Group Profile)" on page 28.
- To change a group profile, use the ALTGROUP command as described in "ALTGROUP (Alter Group Profile)" on page 86.
- To connect a user to a group, use the CONNECT command as described in "CONNECT (Connect User to Group)" on page 128.
- To delete a group profile, use the DELGROUP command as described in "DELGROUP (Delete Group Profile)" on page 141.
- To list a group profile, use the LISTGRP command as described in "LISTGRP (List Group Profile)" on page 172.

Authorization Required

To use the REMOVE command, one of the following conditions must be true:

- You have the SPECIAL attribute
- The group profile is within the scope of a group in which you have the group-SPECIAL attribute
- You are the owner of the group
- You have JOIN or CONNECT authority in the group.

Note: If you only have ownership of the user's profile, you do not have sufficient authority to remove the user from a group.

Syntax

The OWNER operand used with the REMOVE command applies to z/OS systems only. In addition on z/OS, REMOVE can assign a new owner to each group dataset profile currently owned by the user being removed.

The complete syntax of the command is:

REMOVE RE	(***userid ...***) [GROUP(*group-name*)]
z/OS Specific Operand:	[OWNER(*userid or group-name*)]

Parameters

userid
specifies the user you want to remove from the group. If you are removing more than one user from the group, you must enclose the list of user IDs in parentheses.

This value is required and must be the first operand following REMOVE.

GROUP(*group-name*)
specifies the group from which the user is to be removed. If you omit this operand, the default is your current connect group. The value specified for *group-name* cannot be the name of user's default group.

OWNER(*userid* or *group-name*)
Note: *This operand applies to z/OS systems only.*

OWNER specifies a RACF-defined user or group that will own the group data set profiles now owned by the user to be removed.

If you omit this operand when group data set profiles exist that require a new owner, RACF does not remove the user from the group. (Group data set profiles are data set profiles whose names are qualified by the group name or begin with the value supplied by an installation exit.)

The new owner of the group data set profiles must have at least USE authority in the specified group. Do not specify a user who is being removed from the group as the new data set profile owner.

Examples

Example 1

Operation: User WJE10 wants to remove users AFG5 and GMD2 from group PAYROLL.

Known: User WJE10 has JOIN authority to group PAYROLL. User WJE10 is currently connected to group PAYROLL. On z/OS, users AFG5 and GMD2 are connected to group PAYROLL but do not own any group data set profiles, and group PAYROLL is not their default group. On z/VM, users AFG5 and GMD2 are connected to group PAYROLL, but group PAYROLL is not their default group.

Command:
```
REMOVE (AFG5 GMD2)
```

Defaults: GROUP(PAYROLL)

REMOVE Example for z/OS:

Example 2

Operation: User WRH0 wants to remove user PDJ6 from group RESEARCH, assigning user DAF0 as the new owner of PDJ6's group data set profiles.

Known: User WRH0 has CONNECT authority to group RESEARCH. User WRH0 is not logged on to group RESEARCH. User PDJ6 is connected to group RESEARCH and owns group data set profiles (PDJ6's default connect group is not RESEARCH). User DAF0 is connected to group RESEARCH with USE authority.

Command:
```
REMOVE PDJ6 GROUP(RESEARCH) OWNER(DAF0)
```

Defaults: None

RLIST (List General Resource Profile)

System environment

This command applies to both z/OS and z/VM systems.

Purpose

Use the RLIST command to display information on resources belonging to classes specified in the class descriptor table. Note that the DATASET, USER, and GROUP classes are not defined in the class descriptor table.

If you use RLIST for the FILE or DIRECTRY classes, the profile name entered must be in RACF format, rather than SFS format. The LFILE or LDIRECT commands use the SFS format for the profile name and display the same information as RLIST. For the format of these profile names, see "Profile Names for SFS Files and Directories" on page 342.

RACF uses the class descriptor table to determine if a class is defined to RACF, the syntax of resource names within the class, and whether the class is a resource grouping class.

Profiles are listed in alphabetical order. Generic profiles are listed in the same order as they are searched for a resource match. (This also applies to the names in the global access table.)

Note: RACF interprets dates with 2 digit years in the following way, YY represents the 2 digit year.

```
IF 70 < YY <= 99 THEN
   The date is interpreted as 19YY
IF 00 <= YY <= 70 THEN
   The date is interpreted as 20YY
```

Related Commands

- To list an SFS directory profile, use the LDIRECT command as described in "LDIRECT (List SFS Directory Profile)" on page 148.
- To list an SFS file profile, use the LFILE command as described in "LFILE (List SFS File Profile)" on page 154.
- To list a data set profile, use the LISTDSD command as described in "LISTDSD (List Data Set Profile)" on page 160.
- To list a user profile, use the LISTUSER command as described in "LISTUSER (List User Profile)" on page 179.
- To list a group profile, use the LISTGRP command as described in "LISTGRP (List Group Profile)" on page 172.

Comments

This command lists the information in an existing profile for the resource or resource group.

The details that are given for each profile are:

- The resource class
- The name of the resource
- The cross-reference class name (that is, the member class name for resource groups or the group name for non-group resources)
- If the resource named in the command (in the resource-name operand) is a resource group, RACF lists member resources
- For member resources, RACF lists the names of all resource group members in which the entity is a member

- The level of the resource
- The owner of the resource
- The type of access attempts (as specified by the AUDIT operand on the RDEFINE or RALTER command) that are being logged on the SMF data set for z/OS or the SMF data file for z/VM
- The user, if any, to be notified when RACF uses this profile to deny access to the resource
- The universal access authority for the resource
- Your highest level of access authority to the resource
- The installation-defined data (information specified in the DATA operand of the RALTER or RDEFINE commands)

  If your installation is configured to be a B1 security environment, this information will not be listed in your output. * SUPPRESSED * will appear under the installation data field. Only those with system SPECIAL will be allowed to list the field.
- The APPLDATA value, if any

  If your installation is configured to be a B1 security environment, this information will not be listed in your output. * SUPPRESSED * will appear under the application data field. Only those with system SPECIAL will be allowed to list the field.
- The type of access attempts (as specified by the GLOBALAUDIT operand on the RALTER command) that RACF logs
- The status of the WARNING/NOWARNING indicator
- On z/OS, for resources in the TAPEVOL class:
  - The volumes in a tape volume set
  - Whether the TAPEVOL profile is automatic or non-automatic
  - Whether or not the volume can hold more than one data set
  - Whether or not the volume contains a TVTOC.

Additional details:

You can request the following details by using the appropriate RLIST operands:

- The security label, the security level and categories

  (see the AUTHUSER operand)
- The number of times the resource was accessed by all users for each of the following access authorities[8]

  ALTER, CONTROL, UPDATE, READ

  (See the STATISTICS operand)
- Historical data, such as:
  - Date the resource was defined to RACF
  - Date the resource was last referenced [8]
  - On z/OS, date the resource was last accessed at the update level, for DASDVOL and TAPEVOL classes only [8]

  (see the HISTORY operand)
- The standard access list, which displays:
  - All users and groups authorized to access the resource
  - The level of authority for each user and group

[8] This detail is only meaningful when your installation is gathering resource statistics. For a generic profile, RACF replaces any statistics line with NOT APPLICABLE FOR GENERIC PROFILE.

  - The number of times each user has accessed the resource[9].

  (see the AUTHUSER operand)
- The conditional access list, which displays the same fields as the standard access list, as well as the following additional fields:
  - The class of the resource
  - The entity name of the resource.

  (see the AUTHUSER operand)
- On z/OS, for a tape volume that contains RACF-protected data sets, the following information about each RACF-protected data set on the volume:
  - The name used to create the data set
  - The internal RACF name for the data set
  - The volumes on which the data set resides
  - The file sequence number for the data set
  - The date when the data set was created
  - Whether the data set profile is discrete or generic.

  (see the TVTOC operand)
- The contents of the SESSION segment (see the SEGMENT operand)
- The contents of the SSIGNON segment (see the SSIGNON operand)
- The contents of the DLFDATA segment (see the DLFDATA operand).

Authorization Required

You must have a sufficient level of authority for each resource or resource group listed as the result of your request so that one of the following conditions is met:

- You have the SPECIAL attribute.
- The resource profile is within the scope of a group in which you have the group-SPECIAL attribute.
- You have the OPERATIONS attribute.
- The resource profile is within the scope of a group in which you have the group-OPERATIONS attribute.
- You have the AUDITOR or ROAUDIT attribute.
- The resource profile is within the scope of a group in which you have the group-AUDITOR attribute.
- You are the owner of the resource.
- To list the DLFDATA, SESSION, or SSIGNON segments, you must have the SPECIAL, AUDITOR, or ROAUDIT attribute, or your installation must permit you to do so through field-level access checking.
- You are on the access list for the resource and you have at least READ authority. (If your level of authority is NONE, the resource is not listed.)

  If you specify ALL, RACF lists only information pertinent to your user ID.
- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is in the access list and has at least READ authority. (If any group that RACF checked has a level of authority of NONE, the resource is not listed.)
- The universal access authority of the resource is at least READ.
- You have at least read access for the profile name from the GLOBAL ENTRY TABLE (if this table contains an entry for the profile).

[9] This detail is only meaningful when your installation is gathering resource statistics. This detail is not included in the output for generic profiles.

You will see the type of access attempts, as specified by the GLOBALAUDIT operand, only if you have the AUDITOR or ROAUDIT attribute or if the resource profile is within the scope of a group in which you have the group-AUDITOR attribute.

Listing Resource Access Lists

When you are requesting to see the access list for a resource with the AUTHUSER operand, your level of authority is checked for each resource. Your level of authority must be such that one of the following conditions is met:

- You have the SPECIAL attribute.
- The resource profile is within the scope of a group in which you have the group-SPECIAL attribute.
- You have the OPERATIONS attribute.
- The resource profile is within the scope of a group in which you have the group-OPERATIONS attribute.
- You are the owner of the resource.
- You have the AUDITOR or ROAUDIT attribute.
- The resource profile is within the scope of a group in which you have the group-AUDITOR attribute.
- You have alter access for the profile name from the GLOBAL ENTRY TABLE (if this table contains an entry for the profile).
- You are on the access list for the resource and you have ALTER authority. (If you have any other level of authority, you may not use the operand.)
- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is in the access list and has ALTER authority. (If any group that RACF checked has any other level of authority, you may not use the operand.)
- The universal access authority of the resource is ALTER.

Syntax

The following operands used with the RLIST command apply to z/OS systems only:

- TVTOC
- DLFDATA

The complete syntax of the command is:

RLIST	***class-name***
RL	{(***profile-name ...***) | * }
	[ALL]
	[AUTHUSER]
	[{GENERIC | NOGENERIC}]
	[HISTORY]
	[NORACF]
	[RESGROUP]
	[SESSION]
	[SSIGNON]
	[STATISTICS]
z/OS Specific	
Operand:	[DLFDATA]
	[TVTOC]

Parameters

class-name
specifies the name of the class to which the resource belongs. Valid class names are those specified in the class descriptor table (CDT). For a list of general resource classes supplied by IBM, see Appendix B, "IBM-Supplied Resource Classes that Apply to z/VM Systems," on page 349.

This operand is required and must be the first operand following RLIST.

On z/OS, if you specify a class that allows resource names to contain any character (ICHERCDE with OTHER=ANY), resources in the DATASET class that begin with the same first four characters as this class name will also be listed.

(*profile-name ...*) | *

(*profile-name...*)
specifies the name of an existing discrete or generic profile about which information is to be displayed.

The variable *profile-name* or an asterisk (*) is required and must be the second operand following RLIST.

If you specify more than one value for *profile-name*, the list of names must be enclosed in parentheses.

If you specify the profile in the FILE or DIRECTRY class, the profile-name must be in RACF format, not SFS format. For the format of these profile names, see "Profile Names for SFS Files and Directories" on page 342.

On z/OS, if the resource specified is a tape volume serial number that is a member of a tape volume set, information on all the volumes in the set will be displayed.

RACF processes each resource you specify independently. If an error occurs while processing a resource, RACF issues a message and continues processing with the next resource.

*****
specifies that you want to display information for all resources defined to the specified class for which you have the proper authority.

An asterisk or *profile-name* is required and must be the second operand following RLIST.

RACF processes each resource independently and displays information only for those resources for which you have sufficient authority.

If you have the AUDITOR or ROAUDIT attribute, or if the resource profile is within the scope of a group in which you have the group-AUDITOR attribute, RACF displays GLOBALAUDIT information for all resources in the class.

ALL
specifies that you want all information for each resource displayed at your terminal. The access list is not included unless you have sufficient authority to use the AUTHUSER operand (see "Authorization Required" on page 250). The type of access attempts (as specified by the GLOBALAUDIT operand) that are being logged on the SMF data set for z/OS or the SMF data file for z/VM is not included unless you have the AUDITOR or ROAUDIT attribute or the resource profile is within the scope of a group in which you have the group-AUDITOR attribute.

AUTHUSER
specifies that you want the following information included in the output:

- The user categories authorized to access the resource
- The security level required to access the resource
- The security label required to access the resource

[10] This detail is only meaningful when your installation is gathering resource statistics. This detail is not included in the output for generic profiles.

- The standard access list. This includes the following:
  - All users and groups authorized to access the resource
  - The level of authority for each user and group
  - The number of times the user has accessed the resource[10]
- The conditional access list. This list consists of the same fields as in the standard access list, as well as the following fields:
  - The class of the resource via which each user and group in the list can access the target resource of the command. For example, if a user can access the target resource via terminal TERM01, then TERMINAL would be the class listed.
  - The entity name of the resource via which each user and group in the list can access the target resource of the command. In the example above, TERM01 would be listed.

You must have sufficient authorization to use the AUTHUSER operand (see "Authorization Required" on page 250).

DLFDATA

Note: *This operand applies to z/OS systems only.*

specifies that you want to list the contents of the DLFDATA segment for profiles in the DLFCLASS class.

GENERIC | NOGENERIC

If neither operand is specified, RACF lists information for the discrete resource name that matches the resource name you specify. If there is no matching discrete profile, RACF will list the generic profile that most closely matches the resource name.

If asterisk (*) is specified instead of the profile name:

- If GENERIC is specified, all generic profiles will be listed
- If NOGENERIC is specified, all discrete profiles will be listed
- If neither is specified, all discrete and generic profiles will be listed.

GENERIC
specifies that you want RACF to display information for the generic profile that most closely matches a resource name. If you specify GENERIC, RACF ignores a discrete profile that protects the resource.

NOGENERIC
specifies that you want RACF to display information for the discrete profile that protects a resource.

When specifying GENERIC or NOGENERIC, consider the following:

- If you enter

```
RLIST  VMMDISK *
```

RACF lists all discrete and generic profiles in the VMMDISK class

- If you enter

```
RLIST VMMDISK * GENERIC
```

RACF lists information for all the generic profiles in the VMMDISK class.

- If you enter

```
RLIST JESSPOOL * NOGENERIC
```

RACF lists all discrete profiles in the JESSPOOL class.

- If you enter

```
RLIST APPCLU ABC.DEF GENERIC
```

RACF displays the best-fit generic profile that protects the resource ABC.DEF. RACF will ignore discrete profile ABC.DEF if it exists.

HISTORY

specifies that you want to list the following data:

- The date each profile was defined to RACF
- The date each profile was last referenced[11]
- The date of last RACROUTE REQUEST=AUTH for UPDATE authority[11]

NORACF
specifies that you want to suppress the listing of RACF segment information. If you specify NORACF, you must include either the SESSION, DLFDATA, or SSIGNON operand, or a combination.

If you do not specify NORACF, RACF displays the information in the RACF segment of a general resource profile.

The information displayed as a result of using the NORACF operand is dependent on other operands used in the command. For example, if you use NORACF with SESSION also specified, only the SESSION information will be displayed.

RESGROUP
requests a list of all resource groups of which the resource specified by the *profile-name* operand is a member.

If a profile does *not* exist for the specified resource, RACF lists the names of all resource groups of which the resource is a member and to which the command user is authorized. If a profile *does* exist for the specified resource and the command user has ALTER authority to the resource, RACF lists the names of all groups of which the resource is a member.

If a profile *does* exist for the specified resource but the command user has less than ALTER authority to the resource, RACF lists the names of all groups of which the resource is a member and to which the command user is authorized (SPECIAL attribute, profile owner, or at least READ authority).

When *profile-name* is the name of a protected resource (such as a terminal or DASD volume) and *class-name* is a "member class" (such as TERMINAL or DASDVOL), the RESGROUP operand lists the profiles that protect the resource (for example, profiles in the GTERMINL or GDASDVOL class).

This operand applies only to "member classes" for which resource group profiles exist.

SESSION
specifies that the contents of the SESSION segment are to be listed for profiles in the APPCLU class.

SSIGNON
indicates that you want to display the secured signon information.

Note: The secured signon application key value cannot be displayed. However, information is displayed that describes whether the key value is masked or encrypted.

STATISTICS
specifies that you want to list the statistics for each resource. The list will contain the number of times the resource was accessed by users with READ, UPDATE, CONTROL, and ALTER authorities. A separate total is given for each authority level.

[11] These details are only meaningful when your installation is gathering resource statistics. For a generic profile, RACF replaces any statistics line with NOT APPLICABLE FOR GENERIC PROFILE.

Note: This detail is only meaningful when your installation is gathering resource statistics. For a generic profile, RACF replaces any statistics line with `NOT APPLICABLE FOR GENERIC PROFILE`.

TVTOC

Note: *This operand applies to z/OS systems only.*

specifies that you want to see information about the data sets defined in the TVTOC of a TAPEVOL profile. The output displays:

- The name used to create the data set
- The internal RACF name for the data set
- The volumes on which the data set resides
- The file sequence number for the data set
- The date when the data set was created
- Whether the data set profile is discrete or generic.

Examples

Example 1

Operation: User RV2 wants to list all information about the tape volume VOL001.

Known: User RV2 is the owner of tape volume VOL001. User RV2 has the AUDITOR attribute.

Command:
```
RLIST TAPEVOL VOL001 ALL
```

Defaults: None

Output: See Figure 22 on page 257.

Example 2

Operation: User ADM1 wants to list information about the generic profile T* in the TIMS class.

Known: User ADM1 has the SPECIAL and AUDITOR attributes.

Command:
```
RLIST TIMS T*
```

Defaults: None

Output: See Figure 23 on page 258.

RLIST Examples for z/VM:

Example 3

Operation: User VMADM1 wants to list all information about the discrete profile ABC.191 in the VMMDISK class.

Known: User VMADM1 has the SPECIAL and AUDITOR attributes.

Command:
```
RLIST VMMDISK ABC.191 ALL
```

Defaults: None

Output: See Figure 24 on page 259.

Example 4

Operation: On a VM/ESA system, user VMADM2 wants to list information about the auditing and controlling of z/VM events defined in the VMXEVENT profile EVENTS1.

Known: User VMADM2 has the system SPECIAL or system AUDITOR attribute.

Command:
```
RLIST VMXEVENT EVENTS1
```

Defaults: None

Output: See Figure 25 on page 260.

Example 5

Operation: The security administrator wants to display secured signon key information for profile name TSOR001 in the PTKTDATA class to be certain that the application key is masked instead of encrypted.

Known: SIVLE1 is the user ID of the security administrator and has the SPECIAL attribute.

Command:
```
RLIST PTKTDATA TSOR001 SSIGNON
```

Defaults: None

Output: See Figure 26 on page 260.

Example 6

Operation: The security administrator wants to display secured signon key information for profile name TSOR004 in the PTKTDATA class and to be certain that the application key is encrypted instead of masked.

Known: NONNEL is the user ID of the security administrator and has the SPECIAL attribute.

Command:
```
RLIST PTKTDATA TSOR004 SSIGNON
```

Defaults: None

Output: See Figure 27 on page 260.

```
RLIST TAPEVOL VOL001 ALL
CLASS      NAME
-----      ----
TAPEVOL    VOL001

LEVEL  OWNER     UNIVERSAL ACCESS  YOUR ACCESS    WARNING
-----  -----     ----------------  ---- ------    -------
 00    RV2            READ            ALTER         NO

INSTALLATION DATA
-----------------
NONE

APPLICATION DATA
----------------
NONE

SECLEVEL
----------------
NO SECLEVEL

CATEGORIES
----------------
NO CATEGORIES

SECLABEL
----------------
NO SECLABEL

AUDITING
--------
SUCCESS(READ),FAILURES(UPDATE)

GLOBALAUDIT
-----------
ALL(CONTROL)

AUTOMATIC   SINGLE DATA SET
---------   ---------------
   NO             NO

NOTIFY
------
NO USER TO BE NOTIFIED

CREATION DATE  LAST REFERENCE DATE  LAST CHANGE DATE
 (DAY) (YEAR)       (DAY) (YEAR)     (DAY) (YEAR)
-------------  -------------------  ----------------
  146    82          146    82        146    82

ALTER COUNT   CONTROL COUNT   UPDATE COUNT   READ COUNT
-----------   -------------   ------------   ----------
  000000         000000         000005         000000

USER      ACCESS   ACCESS COUNT
----      ------   ------------
RV2       ALTER       000000
ESH25     READ        000000

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

NO TVTOC INFORMATION AVAILABLE
```

Figure 22. Example 1: Output for the RLIST Command

```
RLIST TIMS T*
CLASS      NAME
-----      ----
TIMS       T* (G)

GROUP   CLASS   NAME
-----   -----   ----
GIMS

RESOURCE GROUPS
-------- ------
NONE

LEVEL  OWNER      UNIVERSAL ACCESS  YOUR ACCESS    WARNING
-----  --------   ----------------  ---- ------    -------
 00    ADM1            NONE            ALTER         NO

INSTALLATION DATA
-----------------
NONE

APPLICATION DATA
----------------
REVERIFY

AUDITING
--------
NONE

GLOBALAUDIT
-----------
SUCCESS(UPDATE),FAILURES(READ)

NOTIFY
------
NO USER TO BE NOTIFIED
```

Figure 23. Example 2: Output for the RLIST Command

```
RLIST VMMDISK ABC.191 ALL
CLASS      NAME
-----      ----
VMMDISK    ABC.191

LEVEL  OWNER      UNIVERSAL ACCESS  YOUR ACCESS    WARNING
-----  -------    ----------------  ---- ------    -------
 00    VMADM1          NONE            ALTER         NO

INSTALLATION DATA
-----------------
NONE

APPLICATION DATA
----------------
NONE

SECLEVEL
--------
NO SECLEVEL

CATEGORIES
----------
NO CATEGORIES

SECLABEL
--------
NO SECLABEL

AUDITING
--------
NONE

NOTIFY
------
NO USER TO BE NOTIFIED

CREATION DATE  LAST REFERENCE DATE  LAST CHANGE DATE
 (DAY) (YEAR)       (DAY) (YEAR)      (DAY) (YEAR)
-------------  ------------------  ---------------
  146    82          146    82         146    82

ALTER COUNT   CONTROL COUNT   UPDATE COUNT   READ COUNT
-----------   -------------   ------------   ----------
  000000         000000         000000         000000

USER      ACCESS   ACCESS COUNT
----      ------   ------ -----
VMADM1    ALTER       000000

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

Figure 24. Example 3: Output for the RLIST Command

```
RLIST VMXEVENT EVENTS1
CLASS      NAME
-----      ----
VMXEVENT    EVENTS1

MEMBER CLASS NAME
------ ----- ----
VXMBR

OPTION  z/VM EVENT AUDIT AND/OR CONTROL MEMBERS
------  -----------------------------------
AUDIT   ATTACH
AUDIT   CLOSE
AUDIT   TRANSFER.G

LEVEL  OWNER      UNIVERSAL ACCESS  YOUR ACCESS  WARNING
-----  --------   ----------------  ---- ------  -------
 00    VMADM2          NONE              ALTER    NO

INSTALLATION DATA
-----------------
NONE

APPLICATION DATA
----------------
NONE

AUDITING
--------
NONE

GLOBALAUDIT
-----------
NONE

NOTIFY
------
NO USER TO BE NOTIFIED
```

Figure 25. Example 4: Output for the RLIST Command

```
     SSIGNON INFORMATION

     -------------------

     KEYMASKED DATA IS NOT DISPLAYABLE
```

Figure 26. Example 5: Output for RLIST Command with Encrypted Application Key

```
     SSIGNON INFORMATION

     -------------------

     KEYENCRYPTED DATA IS NOT DISPLAYABLE
```

Figure 27. Example 6: Output for RLIST Command with Masked Application Key

RVARY (Change Status of RACF Database)

System environment

This command applies to both z/OS and z/VM systems.

RACF automatically propagates the RVARY command to all RACF servers that run on the same z/VM system, and to all RACF servers that run on other systems in the same SSI cluster as the issuing system. RACF does not automatically propagate the RVARY command to z/VM systems that share the RACF database outside of an SSI cluster. You must issue the RVARY command separately for each system or restart the RACF servers on the other system or IPL the other system.

Purpose

Use the RVARY command to:

- Deactivate and reactivate the RACF function.
- Switch from using a specific primary database to using its corresponding backup database, perhaps because of a failure related to the primary database.
- Deactivate or reactivate primary or backup RACF databases. (Deactivating a specific primary database causes all RACF requests for access to that database to fail. Deactivating a specific backup database causes RACF to stop duplicating information on that database.)
- Deactivate protection for any resources belonging to classes defined in the CDT while RACF is inactive.

While RACF is deactivated, utilities may be run to diagnose and repair logical errors in the RACF database. RACF installation exits can provide special handling for requests to access RACF-protected resources (for example, by prompting the operator to allow or deny access). If the RACF data set is itself RACF-protected, RACF failsoft processing, which can include installation exit routine processing, controls access to the RACF database. On z/VM, if RACF has been deactivated through RVARY and you wish users to log on using CP directory passwords, you must also issue the SETRACF INACTIVE command.

When RACF is inactive, failsoft processing takes effect. See *z/VM: RACF Security Server System Programmer's Guide* for more information on failsoft processing and using RVARY.

RACF logs each use of the RVARY command provided that the system has been IPLed with RACF active and the use of RVARY changes the status of RACF. For example, if you issue RVARY to deactivate a RACF database that is already inactive, you do not change the status of RACF. Therefore, RACF does not log this particular use of RVARY.

Related Commands

To activate or deactivate RACF, use the SETRACF command as described in “SETRACF (Deactivate/Reactivate RACF on z/VM)” on page 286.

Authorization Required

No special authority is needed to issue the RVARY command. However, the operator (at the operator console or security console) must approve a change in RACF status or the RACF databases before RACF allows the command to complete. If the RVARY command changes RACF status to active or inactive, the operator, to approve the change, must supply an installation-defined password in response to message ICH702A. If the RVARY command changes the RACF databases, the operator, to approve the change, must supply an installation-defined password in response to message ICH703A. See "RVARY Password Considerations " in *z/VM: RACF Security Server System Programmer's Guide*.

Syntax

The INACTIVE(NOTAPE) operand combination used with the RVARY command applies to z/OS systems only:

The complete syntax of the command is:

```
RVARY          [ ACTIVE | INACTIVE
                        [NOCLASSACT(class-name-list | *)
                        (NOTAPE) ] | SWITCH ]
               [ DATASET(data-base-namelist | *) ]
               [ LIST | NOLIST ]
```

Parameters

ACTIVE | INACTIVE [(NOTAPE)] | SWITCH

ACTIVE
specifies that the RACF function for, and access to, the primary RACF databases is to be reactivated.

It is recommended that you use the SETRACF INACTIVE command to deactivate RACF.

If you wish to reactivate a particular primary database or if you wish to activate or reactivate a backup database, then you must specify the DATASET operand with the appropriate database name.

When you reactivate any RACF database it is automatically reallocated.

INACTIVE
specifies that the RACF function for, and access to, the primary RACF databases is to be deactivated. In a multiple service machine environment, if you use RAC to direct an RVARY INACTIVE command to a service machine that has not been assigned to you at LOGON, all subsequent RAC requests sent to that service machine will fail. As a result, you will not be able to direct an RVARY ACTIVE command back to that service machine; to reactivate RACF on that service machine, it must be reinitialized. For an explanation of the issues involved, see the description for message RPIRAC009W (or RPIRAC010W for an SSI cluster environment).

To deactivate a particular primary database or a backup database, you must specify the DATASET operand with the appropriate database name.

When you deactivate any RACF database it is automatically deallocated.

INACTIVE, NOCLASSACT(*class-namelist* | *)
NOCLASSACT specifies those classes for which RACF protection is not in effect while RACF is inactive. Classes you name on NOCLASSACT have no protection in effect. NOCLASSACT(*) indicates that the operand applies to all classes defined in the RACF class descriptor table (CDT). The variable *class-namelist* may contain any class defined in the CDT.

INACTIVE (NOTAPE)
Note: *This operand applies to z/OS systems only.*

NOTAPE specifies that tape volume protection for volumes with IBM standard labels, ANSI labels, and non-standard labels is no longer in effect. This option takes effect immediately and is valid for the current IPL or until RVARY ACTIVE is issued.

SWITCH
specifies that all processing is to switch from the primary RACF databases (identified by the DATASET operand) to the corresponding backup databases. When the switch occurs, the primary databases are deactivated and deallocated. If you specify DATASET(*) or omit DATASET, the command applies to all primary databases. If you specify the name of a backup database on the DATASET operand, RACF ignores it. In order for the switch to take place, the corresponding backup databases must be active.

When you issue RVARY SWITCH, RACF will associate a set of buffers with the new primary database (the old backup database) and disassociate the buffers from the old primary database (the new backup database).

To return to the original primary database, you must first activate the backup databases (the former primary databases) using an RVARY ACTIVE command. An RVARY SWITCH will then return the primary databases to their original position.

DATASET(*data-base-namelist* | *)
specifies a list of one or more RACF databases to be switched, reactivated, or deactivated, depending on the SWITCH, ACTIVE, or INACTIVE operands. If you specify DATASET(*) or omit DATASET, the command applies to all primary databases.

Do not enclose *data-base-namelist* in single quotation marks.

LIST | NOLIST

LIST
specifies that RACF database status information is to be listed for all RACF databases. If you specify ACTIVE, INACTIVE or SWITCH, then the status displayed is the status after the requested changes have been made if the changes were approved by the operator. The LIST command itself does not require operator approval. LIST is the default.

The volume information will contain an *NA if the device on which the RACF database resides has been dynamically reconfigured from the system.

NOLIST
specifies that status information for RACF databases is not to be listed.

Examples

Example 1

Operation: User wants to see if the backup databases are activated.

Command:
```
RVARY LIST
```

Output: See Figure 28 on page 264.

Defaults: None

Example 2

Operation: User wants to activate the backup database RACF.BACK1

Known: The backup database RACF.BACK1 is inactive.

Command:
```
RVARY ACTIVE DATASET(RACF.BACK1)
```

Output: See Figure 29 on page 264.

Defaults: LIST

Example 3

Operation: User wants to switch from using the primary database to using the backup database.

Known: The appropriate backup database is active.

Command:
```
RVARY SWITCH DATASET(RACF.PRIM1)
```

Output: See Figure 30 on page 264.

Defaults: LIST

RVARY Example for z/OS:

Example 4

Operation User WJE10 wants to temporarily deactivate and deallocate RACF in order to make repairs to the RACF database. WJE10 does not want RACF tape volume protection to be enforced while RACF is inactive.

Known The security operator has been informed by the security administrator that a change of RACF status will be requested.

Command `RVARY INACTIVE, NOCLASSACT(TAPEVOL)`

Defaults LIST

```
ICH15013I  RACF DATABASE STATUS:

           ACTIVE  USE   NUMBER  VOLUME    DATASET
           ------  ---   ------  ------    -------
           YES     PRIM    1     D94RF1    RACF.PRIM1
           NO      BACK    1     D94RF1    RACF.BACK1
           YES     PRIM    2     D94RF1    RACF.PRIM2
           NO      BACK    2     D94RF1    RACF.BACK2
           YES     PRIM    3     D94RF1    RACF.PRIM3
           NO      BACK    3     D94RF1    RACF.BACK3
```

Figure 28. Example 1: Output for the RVARY LIST Command

```
ICH15013I  RACF DATABASE STATUS:

           ACTIVE  USE   NUMBER  VOLUME    DATASET
           ------  ---   ------  ------    -------
           YES     PRIM    1     D94RF1    RACF.PRIM1
           YES     BACK    1     D94RF1    RACF.BACK1
           YES     PRIM    2     D94RF1    RACF.PRIM2
           NO      BACK    2     D94RF1    RACF.BACK2
           YES     PRIM    3     D94RF1    RACF.PRIM3
           NO      BACK    3     D94RF1    RACF.BACK3
```

Figure 29. Example 2: Output following the Activation of RACF.BACK1

```
ICH15013I  RACF DATABASE STATUS:

           ACTIVE  USE   NUMBER  VOLUME    DATASET
           ------  ---   ------  ------    -------
           YES     PRIM    1     D94RF1    RACF.BACK1
           YES     BACK    1     D94RF1    RACF.PRIM1
           YES     PRIM    2     D94RF1    RACF.PRIM2
           NO      BACK    2     D94RF1    RACF.BACK2
           YES     PRIM    3     D94RF1    RACF.PRIM3
           NO      BACK    3     D94RF1    RACF.BACK3
```

Figure 30. Example 3: Output following the RVARY SWITCH,DATASET(RACF.PRIM1) Command

SEARCH (Search RACF Database)

System environment

This command applies to both z/OS and z/VM systems.

Purpose

Use the SEARCH command to obtain a list of RACF profiles, users, and groups.

You can request one or more of the following:

- Profile names that contain a specific character string
- Profiles for resources that have not been referenced for more than a specific number of days
- Profiles that RACF recognizes as model profiles
- Data set and general resource profiles that contain a level equal to or greater than the level you specify
- User and resource profiles that contain a security label that matches the security label you specify
- User and resource profiles that contain a security level that matches the security level that you specify
- User and resource profiles that contain an access category that matches the access category that you specify.

In addition, on z/OS, you can request one or more of the following:

- Profiles for tape volumes that contain only data sets with an expiration date that matches the criteria you specify
- Profiles for data sets that reside on specific volumes (or VSAM data sets that are cataloged in VSAM catalogs on specific volumes)
- Profiles for tape data sets, non-VSAM DASD data sets, or VSAM data sets.

You can display the selected profile names at your terminal.

You can also format the selected profile names with specific character strings into a series of commands or messages and retain them in a CLIST data set on z/OS or an EXEC file on z/VM.

Note: RACF interprets dates with 2 digit years in the following way, YY represents the 2 digit year.

```
IF 70 < YY <= 99 THEN
   The date is interpreted as 19YY
IF 00 <= YY <= 70 THEN
   The date is interpreted as 20YY
```

Related Commands

- To search SFS file profiles, use the SRFILE command as described in “SRFILE (Obtain a List of SFS File Profiles)” on page 329.
- To search SFS directory profiles, use the SRDIR command as described in “SRDIR (Obtain a List of SFS Directory Profiles)” on page 324.
- To obtain information on general resource profiles, use the RLIST command as described in “RLIST (List General Resource Profile)” on page 248.
- To define a general resource profile, use the RDEFINE command as described in “RDEFINE (Define General Resource Profile)” on page 225.
- To change a general resource profile, use the RALTER command as described in “RALTER (Alter General Resource Profile)” on page 213.
- To delete a general resource profile, use the RDELETE command as described in “RDELETE (Delete General Resource Profile)” on page 244.

- To permit or deny access to a general resource profile, use the PERMIT command as described in "PERMIT (Maintain Resource Access Lists)" on page 202.

Authorization Required

You must have a sufficient level of authority for each profile selected as the result of your request, such that one of the following conditions is met:

- You have the SPECIAL attribute.
- You have the AUDITOR or ROAUDIT attribute.
- The profile is within the scope of a group in which you have either the group-SPECIAL or group-AUDITOR attribute.
- You are the owner of the user's profile if searching for the profile.

RACF Requirements If Using the CLASS Operand: (Not valid for the USER and GROUP classes)

- If the profile is a DASD data set, the high-level qualifier of the data set name (or the qualifier supplied by a command installation exit) is your user ID.
- You are on the access list for the profile and you have at least READ authority.
- Your current connect group (or, if list-of-groups checking is active, any group to which you are connected) is on the access list and has at least READ authority. (If the group's level of authority is NONE, the resource is not selected.)
- You have the OPERATIONS attribute, or the profile is within the scope of a group in which you have the group-OPERATIONS attribute, and the class is DATASET or a general resource class that specifies OPER=YES in the class descriptor table (CDT).
- The universal access authority is at least READ.

RACF Requirements for the USER(*userid*) Operand: To search successfully with the USER operand, you must pass one of the following checks:

- You have the SPECIAL, AUDITOR, or ROAUDIT attribute.
- You are the owner of the specified user profile.
- You enter your own user ID on the USER operand.
- If security levels and security categories are being used on your system, RACF checks your security level and categories against those in the specified user profile.
- You have the group-SPECIAL or group-AUDITOR attribute in a group to which the specified user is connected.

Syntax

The following operands used with the SEARCH command apply to z/OS systems only:

- ALL | MODEL | TAPE | VSAM | NONVSAM
- EXPIRES
- LIST | NOLIST
- VOLUME
- VOLUME(*volume-serial*)

The complete syntax of the command is:

SEARCH SR	[AGE(*number-of-days*)] [{ALL | GENERIC | NOGENERIC | MODEL | TAPE | VSAM | NONVSAM}] [{CATEGORY [(*category-name*)] | EXPIRES(*number-of-days*) | LEVEL(*level-number*) | SECLABEL(*seclabel-name*) | SECLEVEL [(*seclevel-name*)] | WARNING}] [CLASS({DATASET | *class-name*})] [CLIST [('*string-1*' ['*string-2*'])]] [FILTER(*filter-string*)] [{MASK({*char-1* | *}[*,char-2*]) | NOMASK}] [USER(*userid*)]
z/OS Specific Operands:	[{LIST | NOLIST}] [VOLUME] [VOLUME(*volume-serial*)] **Note:** The operands ALL, MODEL, TAPE, VSAM, and NONVSAM apply to z/OS systems only.

Parameters

AGE(*number-of-days*)
specifies the aging factor to be used as part of the search criteria.

Note: This operand works only for discrete profiles and requires that STATISTICS is enabled system-wide.

Only resources that have not been referenced within the specified number of days are selected, unless you specify CLASS(GROUP). In this case, the SEARCH command uses the date on which the group was defined to determine the age.

You can specify up to five digits for *number-of-days*.

ALL | GENERIC | NOGENERIC | MODEL | TAPE | VSAM | NONVSAM

ALL
Note: *This operand applies to z/OS systems only*.

ALL specifies that RACF is to select all data set profiles (tape, VSAM, and non-VSAM DASD) including both generic and discrete profiles. RACF ignores this operand for classes other than DATASET. ALL is the default if you omit VSAM, NONVSAM, TAPE, GENERIC, NOGENERIC, MODEL, and ALL.

GENERIC | NOGENERIC
specifies whether only generic profiles or no generic profiles (that is, only discrete profiles) are to be selected. If neither operand is specified, both profile types are selected.

RACF ignores these operands unless generic profile command processing is enabled.

MODEL
Note: *This operand applies to z/OS systems only*.

MODEL specifies that only data set profiles having the MODEL attribute are to be selected. RACF ignores this operand for classes other than DATASET.

TAPE
Note: *This operand applies to z/OS systems only*.

TAPE specifies that only tape data sets are to be selected. RACF ignores this operand for classes other than DATASET.

VSAM
Note: *This operand applies to z/OS systems only*.

VSAM specifies that only VSAM data sets are to be selected. RACF ignores this operand for classes other than DATASET.

NONVSAM
Note: *This operand applies to z/OS systems only*.

NONVSAM specifies that only non-VSAM data sets are to be selected. RACF ignores this operand for classes other than DATASET.

CATEGORY | EXPIRES | LEVEL | SECLEVEL | SECLABEL | WARNING

CATEGORY[(*category-name*)]
specifies that RACF is to select only profiles with an access category matching the category name that you specify, where *category-name* is an installation-defined name that is a member of the CATEGORY profile in the SECDATA class. If you specify CATEGORY and omit *category-name*, RACF selects only profiles that contain undefined access category names (names that were once known to RACF but that are no longer valid).

RACF ignores this operand when CLASS(GROUP) is specified.

EXPIRES(*number-of-days*)
Note: *This operand applies to z/OS systems only*.

specifies that RACF is to select only tape volumes on which all of the data sets either have expired or will expire within the number of days that you specify. The variable *number-of-days* is a 1-to-5-digit number in the range of 0 through 65533—or for data sets that never expire, 99999. RACF ignores this operand for classes other than TAPEVOL.

LEVEL(*level-number*)
specifies that RACF is to select only profiles with an installation-defined level that equals the level number you specify. You can specify a value for *level* of 0 through 99.

RACF ignores this operand for classes other than DATASET or classes defined in the RACF class descriptor table.

SECLABEL(*seclabel-name*)
specifies that RACF is to select only profiles with a security label name that matches the value you specify for *seclabel*.

SECLEVEL[(*seclevel-name*)]
specifies that RACF is to select only profiles with a security level name that matches *seclevel-name*, where *seclevel-name* is an installation-defined name that is a member of the SECLEVEL profile in the SECDATA class. If you specify SECLEVEL and omit *seclevel-name,* RACF selects only profiles that contain undefined security level names (names that were once known to RACF but that are no longer valid).

RACF ignores this operand when CLASS(GROUP) is specified.

WARNING
specifies that only resources with the WARNING indicator are to be selected.

RACF ignores this operand when you specify CLASS as USER or GROUP.

CLASS(DATASET | *class-name*)
specifies the name of the class of profiles to be searched. The valid resource classes are DATASET, USER, GROUP, and those specified in the class descriptor table (CDT). For a list of general resource classes defined in the IBM-supplied CDT, see Appendix B, “IBM-Supplied Resource Classes that Apply to z/VM Systems,” on page 349.

If you omit this operand, the default value is DATASET.

To search all RACF-defined user profiles, you must have the SPECIAL, AUDITOR, or ROAUDIT attribute.

When searching with the CLASS(GROUP) option, groups will be listed based upon the connect authority of the user, **not** READ or higher access to the profile.

On z/OS, if CLASS(TAPEVOL) is specified, RACF processes all volumes that meet the search criteria independently, even if the volumes belong to a tape volume set.

On z/OS, if you specify a class that allows profile names to contain any character (ICHERCDE with OTHER=ANY), RACF also selects profiles in the DATASET class that begin with the same first 4 characters as this class name and that satisfy the other criteria you specify on this SEARCH command.

CLIST[('*string-1* '[' *string-2*'])]

Note: For z/VM, this operand applies only when the SEARCH command is issued using RACFISPF, and the following description applies only to z/VM.

CLIST specifies that the selected profile names will be saved in the R$CLIST EXEC file on your A disk. One record is put into the file for each selected profile name.

'*string-1*'['*string-2*']
specifies strings of alphanumeric characters that are put into the EXEC records along with the selected profile names. Each string must be enclosed in single quotation marks. In this way, you can build a set of commands that are similar except for the profile name.

The format of the EXEC record is as follows:

```
string-1 profile name string-2
```

If you want a string of data to appear only after the profile name, specify 'string-1' as an empty string (''). If both strings are empty, the EXEC record contains only the profile name.

FILTER(*filter-string*)
(Also see the MASK operand.)

specifies the string of alphanumeric characters used to search the RACF database. The filter string defines the range of profile names you wish to select from the RACF database. For a tape or DASD data set name, the filter string length must not exceed 44 characters. For a general resource class, the filter string length must not exceed the length of the profile name specified in the class descriptor table (CDT).

When you issue the SEARCH command with the FILTER operand, RACF lists profile names from the RACF database matching the search criteria specified in the filter string. Note that RACF lists only those profile names that you are authorized to see.

The following generic characters have special meaning when used as part of the filter string:

%
You can use the percent sign to represent any *one* character in the profile name, including a generic character. For example, if you specify DASD%% as a filter string, it can represent profile names such as DASD01, DASD2A, and DASD%5. If you specify %%%%% as a filter string, it can represent profile names DASD1, DASD2, DASD%, TAPE%, MY%%%, TAPE*, and %%%%*.

*****
You can use a single asterisk to represent *zero or more characters* in a **qualifier**, including generic characters. For example, AB*.CD can represent data set profile names such as AB.CD, ABEF.CD, and ABX.CD. ABC.D* can represent data set profile names such as ABC.DEFG, ABC.D%%%, and ABC.D%*. If you specify a single asterisk as the only character in a qualifier, it represents the entire qualifier. For example, ABC.* represents data set profile names such as ABC.D, ABC.DEF, ABC.%%%, and ABC.%DE. For example, *DASD* can represent profile names such as MYDASD01, ADASD223, and DASD%%*. You can also specify a single asterisk as the only character in the filter-string to represent any general resource profile name. For example, * can represent DASD01, DASD%%*, ABCDEF, %%%, %*, *, and so on.

******

For *general resource* and *data set profile names*, you can use a double asterisk to represent zero or more qualifiers in the profile name. For example, AB.**.CD represents data set profile names such as AB.CD, AB.DE.EF.CD, and AB.XYZ.CD. You cannot specify other characters with ** within a qualifier. (For example, you can specify FILTER(USER1.**), but not FILTER(USER1.A**). You can also specify ** as the only characters in the filter-string to represent any entire data set profile name.

Note:

1. You can use FILTER for an alternative to MASK | NOMASK as a method for searching the RACF database. FILTER offers more flexibility than MASK. For example, when you use FILTER, you can generalize the character string you specify to match multiple qualifiers or multiple characters within a profile name. You can also specify a character string to match a single character regardless of its value or search for a character string anywhere in a profile name.
2. You cannot use a generic character (*, **, or %) in the high-level qualifier when you define a generic profile for a data set. However, you can use a generic character in the high-level qualifier of a data set name when specifying a filter-string with the FILTER operand.
3. The FILTER and MASK | NOMASK operands are mutually exclusive; you cannot specify FILTER with either MASK or NOMASK on the same SEARCH command.

LIST | NOLIST

Note: *These operands apply to z/OS systems only*.

LIST

specifies that the selected data set names, volume serial numbers, or terminal names are to be displayed at your terminal. LIST is the default value when you omit both LIST and NOLIST.

NOLIST

specifies that the selected data set names, volume serial numbers, or terminal names are not to be displayed at your terminal. You can use this operand only when you specify the CLIST operand. If you use NOLIST without CLIST, the command fails.

MASK | NOMASK

MASK(*char-1* | * [, *char-2*])

(Also see the FILTER operand.)

specifies the strings of alphanumeric characters used to search the RACF database. This data defines the range of profile names selected. The two character strings together must not exceed 44 characters for a tape or DASD data set name, or, for general resource classes, the length specified in the class descriptor table.

char-1

Each profile name selected with this command starts with *char-1*. The string may be any length up to the maximum allowable length of the resource name. All profile names beginning with *char-1* are searched.

If an asterisk (*) is specified for *char-1*:

- For DATASET class, your user ID is used as the default value for *char-1*.
- For general resource classes specified in the class descriptor table, *char-1* is ignored, and *char-2* will identify the character string appearing anywhere in the resource name.

char-2

If you specify *char-2*, the selected profile names include only those names containing *char-2* somewhere after the occurrence of *char-1*. This limits the list to some subset of resource names identified with *char-1*.

If you omit both the MASK and NOMASK operands, your user ID is used as the default value for the DATASET class, whereas the entire class is searched for any resource class defined in the class descriptor table. (Note that, for any resource class defined in the class descriptor table, omitting both operands is the same as NOMASK.)

NOMASK
specifies that RACF is to select all profiles (to which you are authorized) in the specified class.

Note: The MASK|NOMASK and FILTER operands are mutually exclusive. You cannot specify MASK or NOMASK with FILTER on the same SEARCH command.

USER(*userid*)
specifies that RACF is to list the profiles that the specified user has access to (READ authority or higher, or owner) for the class you specify on the CLASS operand. RACF lists only those profiles that the specified owner is allowed to see.

If you issue:

```
SEARCH  USER(JONES)  CLASS(ACCTNUM)
```

RACF lists all TSO account numbers that user ID JONES is allowed to use.

If you issue:

```
SEARCH  USER(JONES) NOMASK
```

RACF lists profiles in the DATASET class that JONES has access to.

If you issue:

```
SEARCH  USER(JONES)  CLASS(GROUP)
```

RACF lists all groups that user ID JONES owns or, in which JONES has JOIN or CONNECT authority or the group-SPECIAL attribute.

Note:

1. If you omit the CLASS operand, the default class is DATASET. For more information, see the description of the CLASS operand.
2. You should not specify a user ID that has been revoked. If you need to display information about a user whose user ID is revoked, perform the following steps:
   a. Change the password for the user ID
   b. Resume the user ID
   c. Issue the SEARCH command to display the desired information
   d. Revoke the user ID.
3. You can only specify one user ID at a time on the USER operand. If you need to display information about all users, first create the R$CLIST EXEC by issuing the following command with RACFISPF:

   ```
   SEARCH  CLASS(USER)  CLIST('SEARCH USER(' ')  +
      CLASS(class-name)')
   ```

   After you create the EXEC, execute it to display the desired information.

VOLUME
Note: *This operand applies to z/OS systems only*.

VOLUME specifies that you want RACF to display volume information for each tape or DASD data set that meets the search criteria specified by the MASK or FILTER operand.

RACF ignores this operand if you specify GENERIC.

For non-VSAM data sets, the volume serial number displayed is the location of the data set. For VSAM data sets, the volume serial number displayed is the location of the catalog entry for the data set. For tape data sets, the volume serial number displayed is the location of the TVTOC entry for the date set.

This operand is valid only for CLASS(DATASET). RACF ignores it for all other class values.

VOLUME(*volume-serial ...*)
Note: *This operand applies to z/OS systems only*.

VOLUME(volume-serial...) specifies the volumes to be searched; the volume serial numbers become part of the search criteria. Non-VSAM DASD data sets are selected if they reside on the specified volumes. VSAM data sets are selected if the catalog entries for the data sets reside on the specified volumes. Tape data sets are selected if the TVTOC entries for the data set reside on the specified volumes.

RACF ignores this operand if you specify GENERIC.

If the selected data set names are displayed at your terminal, the volume information is included with each data set name.

This operand is valid only for CLASS(DATASET). RACF ignores it for all other class values.

Examples

Example 1

Operation	User CD0 wants to list all of her RACF data set profiles.
Known	User CD0 is RACF-defined.
Command	SEARCH
Defaults	MASK(CD0) CLASS(DATASET) LIST ALL
Results	A list of all profiles in the DATASET class beginning with “CD0”.

Example 2

Operation	User IA0 wants to remove the RACF profiles for all DATA-type data sets for the group RESEARCH that have not been referenced for 90 days. The user wants an EXEC data set to be created with DELDSD commands for each profile satisfying the search criteria. A list is not desired.
Known	User IA0 is connected to group RESEARCH (and is the owner of all profiles in group RESEARCH) with the group-SPECIAL attribute.
Command	`SEARCH FILTER(RESEARCH.DATA) AGE(90) CLIST('DELDSD ') NOLIST` **or** SEARCH MASK(RESEARCH.DATA) AGE(90) CLIST('DELDSD ') NOLIST
Defaults	CLASS(DATASET) ALL
Results	An EXEC data set with the name IA0.EXEC.RACF.CLIST is built, and the records in it are in the format: `DELDSD 'data-set-name'`

Example 3

Operation: User ADMIN wants to obtain a list of all data set profiles, both discrete and generic, that have the word “DATA” as the second-level qualifier.

Known: User ADMIN has the SPECIAL attribute.

Command:
```
SEARCH FILTER(*.DATA.**)
```

Defaults: CLASS(DATASET) LIST ALL

Results: A list of all profiles in the DATASET class with the word “DATA” as the second-level qualifier. For example, the list might include data sets with names such as RESEARCH.DATA, TEST.DATA, USER.DATA.WEEK1, or GROUP.DATA.TEST.ONE.

Example 4

Operation: User ADM1 wants to obtain a list of all data set profiles, both discrete and generic, having a qualifier (any level) that begins with the word “TEST” and contains only one additional character (such as TEST1, TEST2, or TESTA).

Known: User ADM1 has the SPECIAL attribute.

Command:
```
SEARCH FILTER(**.TEST%.**)
```

Defaults: CLASS(DATASET) LIST ALL

Results: A list of all profiles in the DATASET class having a qualifier of any level that begins with the word “TEST” and contains only one additional character. For example, the list might include data sets with names such as RESEARCH.TEST1, TEST2.DATA, MY.TEST4.DATA, MY.TEST%.* USER.DATA.TEST5, USER.DATA.TEST%.**, or GROUP.DATA.TESTC.FUN.

Example 5

Operation: User ADMIN wishes to find and revoke all user IDs of users who have not accessed the system in the last 90 days. For this to work, the INITSTATS option (specified on the SETROPTS command) must be in effect.

Known: User ADMIN has the SPECIAL attribute.

Command:
```
SEARCH CLASS(USER) AGE(90)
CLIST('ALTUSER ' ' REVOKE')
```

Defaults: Process all user ID entries.

Results: An EXEC data set with the name ADMIN.EXEC.RACF.CLIST listing the user ID for each user that has not accessed the system within 90 days, with records in the following format:

```
ALTUSER  userid  REVOKE
```

Example 6

Operation: User ADM1 wants to get a list of all generic profiles for group SALES.

Known: User ADM1 has the SPECIAL attribute.

Command:
```
SEARCH MASK(SALES.*)
```

Defaults: CLASS(DATASET) LIST ALL

Results: A list of all profiles in the DATASET class beginning with “SALES.*”. (Since the string specified contains an asterisk, this list will consist only of generic profiles.)

Example 7

Operation: User ADM1 wants to get a list of all data set profiles that include a security level of CONFIDENTIAL.

Known: User ADM1 has the SPECIAL attribute. The CONFIDENTIAL security level has been defined to RACF.

Command:
```
SEARCH CLASS(DATASET)
SECLEVEL(CONFIDENTIAL)
```

Defaults: LIST ALL

Results: A list of all profiles in the DATASET class with a security level of CONFIDENTIAL.

SEARCH Examples for z/VM:

Example 8

Operation: User VMCD0 wants to list all of her RACF minidisk profiles.

Known: User VMCD0 is RACF-defined.

Command:
```
SEARCH CLASS(VMMDISK) FILTER(VMCD0.*)
```

or

```
SEARCH CLASS(VMMDISK) MASK(VMCD0)
```

Defaults: None

Results: A list of all profiles in the VMMDISK class beginning with “VMCD0”.

Example 9

Operation: User VMADM1 wants to get a list of all discrete profiles for group SALES.

Known: User VMADM1 has the SPECIAL attribute.

Command:
```
SEARCH CLASS(VMMDISK) FILTER(SALES*)
```

or

```
SEARCH CLASS(VMMDISK) MASK(SALES)
```

Defaults: None

Results: A list of all profiles in the VMMDISK class beginning with “SALES”.

Example 10

Operation: User VMADM1 wants to get a list of all minidisk profiles that include a security level of CONFIDENTIAL.

Known: User VMADM1 has the SPECIAL attribute. The CONFIDENTIAL security level has been defined to RACF.

Command:
```
SEARCH CLASS(VMMDISK)
SECLEVEL(CONFIDENTIAL)
```

Defaults: None

Results: A list of all profiles in the VMMDISK class with a security level of CONFIDENTIAL.

Example 11

Operation: User VMADM1 wants to obtain a list of all RSCS nodes that are protected by RACF.

Known: User VMADM1 has the SPECIAL attribute.

Command:
```
SEARCH CLASS(VMNODE)
```

Defaults: None

Results: A list of all RSCS nodes defined to RACF.

SETEVENT (Set z/VM Events)

System environment

This command applies to z/VM systems only.

The SETEVENT command provides an installation with a system-wide ability and a user-specific ability to control and to audit z/VM events. z/VM events include DIAGNOSE codes, CP commands, certain events related to communication between virtual machines, and certain spool file activities.

The RDEFINE command creates VMXEVENT profiles, which are stored in the RACF database. The SETEVENT command processes these profiles.

The contents of the profiles are used (by SETEVENT) to set either the system security authorization or the user security authorization in the control program (CP).

The SETEVENT command also lists the z/VM events being audited and controlled.

The documentation has been divided into two parts for clarity and ease of use. Following is the system-wide information for SETEVENT. Also see "Authorization Required" on page 278.

Purpose

Use the SETEVENT command to:

- Change the z/VM events that are audited or controlled by RACF.

  Auditing of all z/VM events is available, and control of some events is available. See *z/VM: RACF Security Server Security Administrator's Guide* for more information on controllable events.
- Prevent users from issuing the DIAL, UNDIAL, and MESSAGE commands before logging on.

  If a user issues DIAL, UNDIAL, or MESSAGE before logging on, no user ID is associated with the request.
- List the following information:
  - What configuration (YES or NO) is in effect for the DIAL, UNDIAL, and MESSAGE commands.
  - What z/VM events are controlled by RACF.
  - What z/VM events are audited by RACF.

Authorization Required

To issue the SETEVENT command, you must have the SPECIAL, AUDITOR, or ROAUDIT attribute.

- If you have SPECIAL:

  You can enter all the operands of the command, but REFRESH will only update the z/VM events that are controlled on the system.
- If you have AUDITOR:

  You can refresh the auditing of z/VM events on the system with the REFRESH operand. If you specify a profile name on the REFRESH operand, you also must be the owner of the profile, or have ALTER authority to the profile.

  You can also use the LIST operand.
- If you have ROAUDIT:

  You can use the LIST operand.

Syntax

The syntax of this command for system-wide operands is:

```
SETEVENT        [ LIST | REFRESH [profile-name] }
                —or—
                [ DIAL | NODIAL ]
                [ PRELOGMSG | NOPRELOGMSG ]
```

Parameters

LIST
specifies that the following information is to be listed:

- Whether users can issue the DIAL, UNDIAL, and MESSAGE commands before logging on
- What z/VM events are controlled by RACF
- What z/VM events are audited by RACF

To obtain a display of SETEVENT LIST output that you can scroll through, use the RACF ISPF panels. To obtain a display of SETEVENT LIST output that is copied to a file, use the RAC command.

If you specify the LIST operand, no other operands can be specified on the command.

REFRESH
specifies that the information stored in the current system z/VM event profile in the RACF database is to be used to refresh the system security authorizations in effect for the audit and control of z/VM events.

If you have a system z/VM event profile in place, this option can be used during IPL to reinstate the options that existed before IPL.

SETEVENT REFRESH commands are automatically propagated to all RACF servers running on the same z/VM system, and to other systems in the same SSI cluster as the issuing system, unless they target specific users by including a profile in the form USERSEL.*userid*.

If you specify the REFRESH operand, no other operands can be specified on the command.

REFRESH *profile-name*
specifies a z/VM system event profile that an installation wants to use to set system options (for the audit and control of z/VM events). The options in the specified profile will replace the options currently in effect on the system (in the system security authorizations).

The z/VM event profile is stored in the RACF database.

The value for *profile-name* must be defined in the VMXEVENT class. Members in the profile define which z/VM events are audited, not audited, controlled, or not controlled. For more information on creating a VMXEVENT profile, see *z/VM: RACF Security Server Security Administrator's Guide*.

If you specify the REFRESH operand, no other operands can be specified on the command.

DIAL | NODIAL
Note: If you specify either DIAL or NODIAL, only PRELOGMSG or NOPRELOGMSG can be also specified in the same command.

DIAL
specifies that users can issue the DIAL or UNDIAL commands before logging on.

NODIAL
specifies that users cannot issue the DIAL or UNDIAL commands before logging on.

PRELOGMSG | NOPRELOGMSG
If you specify either PRELOGMSG or NOPRELOGMSG, only DIAL or NODIAL can be also specified in the same command.

PRELOGMSG
specifies that users can issue the MESSAGE command before logging on.

NOPRELOGMSG
specifies that users cannot issue the MESSAGE command before logging on.

Note: The status of DIAL, UNDIAL, and MESSAGE is updated immediately; a REFRESH is not required.

Authorization Required

Use the SETEVENT command to establish audits and controls unique to an individual user on the system.

By issuing the SETEVENT command with the high-level qualifier USERSEL, individuals can list, refresh, or suspend a user's security authorization.

You must have the SPECIAL and/or AUDITOR attributes to create an individual z/VM event profile.

- If you have SPECIAL:

  You can enter all the operands and refresh and reset the z/VM events controlled in an individual's user security authorization.
- If you have AUDITOR:

  You can enter all the operands and control the auditing of events in the individual's user security authorization.

  In order to refresh and reset an individual's user security authorization, you *must* own the VMXEVENT profile, have ALTER access to the profile, or have CLAUTH to the VMXEVENT class.

Syntax

The syntax of the command for user-specific operands is:

```
SETEVENT        [ LIST USERSEL.userid ]
                —or—
                [ REFRESH USERSEL.userid ]
                —or—
                [ RESET USERSEL.userid ]
```

LIST USERSEL.*userid*
specifies that RACF is to display the contents of the individual's user security authorization.

REFRESH USERSEL.*userid*
specifies that a copy of the individual's user z/VM event profile is being used to refresh the user's security authorization.

The refresh goes into effect immediately; the user must be logged on or disconnected, or an error message is issued.

RESET USERSEL.*userid*
specifies that the individual's user security authorization is to be suspended. Both the auditing and control options are no longer in effect. The individual is subject to the options set in the system security authorization

The reset goes into effect immediately; the user must be logged on or disconnected, or an error message is issued.

The suspension ends when the user logs off. At the next logon, the USERSEL.*userid* profile is again in effect. For information about deleting the USERSEL profile, see *z/VM: RACF Security Server Security Administrator's Guide*.

Examples

SETEVENT Example on z/VM for User-Specific Operands:

Example 1

System **z/VM**

Operation User AUDIT1 wants to suspend individual auditing and individual control for user ID DJONES.

Known User AUDIT1 has the AUDITOR attribute and owns the VMXEVENT profile USERSEL.DJONES.

Command `SETEVENT RESET USERSEL.DJONES`

Result User ID DJONES is now being audited and controlled by the system security authorization. The command temporarily suspends the use of DJONES's user security authorization.

SETEVENT Example on z/VM for System-Wide Operands:

Example 2

System **VM/ESA**

Operation User VMADM1 wants to use VMXEVENT profile EVENTS1 to audit z/VM events on a VM/ESA system.

Known User VMADM1 has the AUDITOR attribute and ALTER authority to profile EVENTS1.

Command `SETEVENT REFRESH EVENTS1`

Output The information that z/VM uses to determine when to call RACF to audit an event is updated using profile EVENTS1.

All the controllable events are being controlled except for MDISK, and a number of the more security-sensitive CP commands are being audited. The controllable events are not being audited here, because auditing can be controlled within the profiles that protect the relevant resources.

Sample Output for SETEVENT LIST from Example 2. This list can change because of product updates. For an accurate and up-to-date list, issue the SETEVENT LIST command.

```
PRE-LOGON COMMANDS

COMMAND              CONFIGURED IN
-------              -------------
DIAL                   YES
MESSAGE.ANY            YES
UNDIAL                 YES


CONTROLLABLE VM EVENTS       CURRENT SYSTEM CONTROL PROFILE: EVENTS1

VM EVENT                     STATUS     VM EVENT                     STATUS
--------                     ------     --------                     ------
COUPLE.G                     CONTROL    FOR.C                        CONTROL
FOR.G                        CONTROL    LINK                         CONTROL
STORE.C                      CONTROL    TAG                          CONTROL
TRANSFER.D                   CONTROL    TRANSFER.G                   CONTROL
TRSOURCE                     CONTROL    DIAG088                      CONTROL
DIAG0A0                      CONTROL    DIAG0D4                      CONTROL
DIAG0E4                      CONTROL    DIAG280                      CONTROL
APPCPWVL                     CONTROL    MDISK                        CONTROL
RSTDSEG                      CONTROL    RDEVCTRL                     CONTROL


AUDITABLE VM EVENTS          CURRENT SYSTEM AUDIT PROFILE: EVENTS1

VM EVENT                     STATUS     VM EVENT                     STATUS
--------                     ------     --------                     ------
ACNT                         NO_AUDIT   ACTIVATE                     NO_AUDIT
ADJUNCT                      NO_AUDIT   ADSTOP                       NO_AUDIT
```

```
ASSOCIATE                NO_AUDIT   AT                       NO_AUDIT
ATTACH                   NO_AUDIT   ATTN                     NO_AUDIT
AUTOLOG.A                NO_AUDIT   AUTOLOG.B                NO_AUDIT
BACKSPACE                NO_AUDIT   BEGIN                    NO_AUDIT
CHANGE.D                 NO_AUDIT   CHANGE.G                 NO_AUDIT
CLOSE                    NO_AUDIT   COMMANDS                 NO_AUDIT
COMMIT                   NO_AUDIT   CONCOPY                  NO_AUDIT
COUPLE.G                 NO_AUDIT   CPACCESS                 NO_AUDIT
CPCACHE                  NO_AUDIT   CPHX                     NO_AUDIT
CPLISTFILE               NO_AUDIT   CPRELEASE                NO_AUDIT
CPFORMAT                 NO_AUDIT   CPTRAP                   NO_AUDIT
CPTYPE                   NO_AUDIT   CPU                      NO_AUDIT
CPVLOAD                  NO_AUDIT   CPXLOAD                  NO_AUDIT
CPXUNLOAD                NO_AUDIT   DEACTIVE                 NO_AUDIT
DEACTIVATE               NO_AUDIT   DEDICATE                 NO_AUDIT
DEFINE.A                 NO_AUDIT   DEFINE.B                 NO_AUDIT
DEFINE.E                 NO_AUDIT   DEFINE.G                 NO_AUDIT
DEFSEG                   NO_AUDIT   DEFSYS                   NO_AUDIT
DELETE                   NO_AUDIT   DESTAGE                  NO_AUDIT
DETACH.B                 NO_AUDIT   DETACH.G                 NO_AUDIT
DIAL                     NO_AUDIT   DISABLE.A                NO_AUDIT
DISABLE.B                NO_AUDIT   DISABLE.F                NO_AUDIT
DISASSOCIATE             NO_AUDIT   DISCARD                  NO_AUDIT
DISCONNECT               NO_AUDIT   DISPLAY.C                NO_AUDIT
DISPLAY.E                NO_AUDIT   DISPLAY.G                NO_AUDIT
DRAIN.B                  NO_AUDIT   DRAIN.D                  NO_AUDIT
DUMP.C                   NO_AUDIT   DUMP.E                   NO_AUDIT
DUMP.G                   NO_AUDIT   DUPLEX                   NO_AUDIT
ECHO                     NO_AUDIT   ENABLE.A                 NO_AUDIT
ENABLE.B                 NO_AUDIT   ENABLE.F                 NO_AUDIT
EXTERNAL                 NO_AUDIT   FLASHCOPY                NO_AUDIT
FLUSH                    NO_AUDIT   FOR.C                    NO_AUDIT
FOR.G                    NO_AUDIT   FORCE                    NO_AUDIT
FORWARD                  NO_AUDIT   FREE.B                   NO_AUDIT
FREE.D                   NO_AUDIT   GIVE                     NO_AUDIT
HALT                     NO_AUDIT   HOLD.B                   NO_AUDIT
HOLD.D                   NO_AUDIT   HYPERSWAP                NO_AUDIT
INDICATE.B               NO_AUDIT   INDICATE.C               NO_AUDIT
INDICATE.E               NO_AUDIT   INDICATE.G               NO_AUDIT
IPL                      NO_AUDIT   LINK                     NO_AUDIT
LOADBUF                  NO_AUDIT   LOADVFCB                 NO_AUDIT
LOCATE.C                 NO_AUDIT   LOCATE.E                 NO_AUDIT
LOCATEVM                 NO_AUDIT   LOCK                     NO_AUDIT
LOGON                    NO_AUDIT   LOGOFF                   NO_AUDIT
MESSAGE.A                NO_AUDIT   MESSAGE.B                NO_AUDIT
MESSAGE.ANY              NO_AUDIT   MODIFY.A                 NO_AUDIT
MODIFY.B                 NO_AUDIT   MONITOR.A                NO_AUDIT
MONITOR.E                NO_AUDIT   MSGNOH                   NO_AUDIT
NOTREADY                 NO_AUDIT   ORDER.D                  NO_AUDIT
ORDER.G                  NO_AUDIT   PURGE.A                  NO_AUDIT
PURGE.B                  NO_AUDIT   PURGE.C                  NO_AUDIT
PURGE.D                  NO_AUDIT   PURGE.E                  NO_AUDIT
PURGE.G                  NO_AUDIT   READY                    NO_AUDIT
RECORDING.A              NO_AUDIT   RECORDING.B              NO_AUDIT
RECORDING.C              NO_AUDIT   RECORDING.E              NO_AUDIT
RECORDING.F              NO_AUDIT   REDEFINE                 NO_AUDIT
REFRESH                  NO_AUDIT   REPEAT                   NO_AUDIT
REQUEST                  NO_AUDIT   RESET.B                  NO_AUDIT
RESET.G                  NO_AUDIT   RESTART.A                NO_AUDIT
RESTART.B                NO_AUDIT   RESTART.G                NO_AUDIT
RETAIN                   NO_AUDIT   REWIND                   NO_AUDIT
SAVESEG                  NO_AUDIT   SAVESYS                  NO_AUDIT
SCREEN                   NO_AUDIT   SEND.C                   NO_AUDIT
SEND.G                   NO_AUDIT   SHUTDOWN                 NO_AUDIT
SIGNAL.A                 NO_AUDIT   SIGNAL.C                 NO_AUDIT
SIGNAL.G                 NO_AUDIT   SILENTLY                 NO_AUDIT
SLEEP                    NO_AUDIT   SMSG                     NO_AUDIT
SNAPDUMP                 NO_AUDIT   SPACE                    NO_AUDIT
SPOOL                    NO_AUDIT   SPXTAPE.D               NO_AUDIT
SPXTAPE.E                NO_AUDIT   SPXTAPE.G               NO_AUDIT
START.B                  NO_AUDIT   START.D                  NO_AUDIT
STOP                     NO_AUDIT   STORE.C                  NO_AUDIT
STORE.G                  NO_AUDIT   SYNCMDRS.A               NO_AUDIT
SYNCMDRS.B               NO_AUDIT   SYNCMDRS.F               NO_AUDIT
SYSTEM                   NO_AUDIT   TAG                      NO_AUDIT
TERMINAL                 NO_AUDIT   TRACE                    NO_AUDIT
TRANSFER.D               NO_AUDIT   TRANSFER.G               NO_AUDIT
TRSAVE.A                 NO_AUDIT   TRSAVE.C                 NO_AUDIT
TRSOURCE                 NO_AUDIT   UNCOUPLE                 NO_AUDIT
UNDEDICATE               NO_AUDIT   UNDIAL                   NO_AUDIT
UNLOCK                   NO_AUDIT   VARY                     NO_AUDIT
VDELETE                  NO_AUDIT   VINPUT                   NO_AUDIT
```

```
VMDUMP                  NO_AUDIT   VMRELOCATE              NO_AUDIT
WARNING.A               NO_AUDIT   WARNING.B               NO_AUDIT
WARNING.C               NO_AUDIT   XAUTOLOG.A              NO_AUDIT
XAUTOLOG.B              NO_AUDIT   XAUTOLOG.G              NO_AUDIT
XLINK.A                 NO_AUDIT   XLINK.B                 NO_AUDIT
XSPOOL.D                NO_AUDIT   XSPOOL.G                NO_AUDIT
QUERY.ABEND             NO_AUDIT   QUERY.ACCOUNT           NO_AUDIT
QUERY.ADJUNCT           NO_AUDIT   QUERY.ALL               NO_AUDIT
QUERY.ALLOC             NO_AUDIT   QUERY.BYUSER.E          NO_AUDIT
QUERY.BYUSER.ANY        NO_AUDIT   QUERY.CACHE             NO_AUDIT
QUERY.CACHEFW           NO_AUDIT   QUERY.CAPABILITY.A      NO_AUDIT
QUERY.CAPABILITY.B      NO_AUDIT   QUERY.CAPABILITY.C      NO_AUDIT
QUERY.CAPABILITY.E      NO_AUDIT   QUERY.CFLINKS.A         NO_AUDIT
QUERY.CFLINKS.B         NO_AUDIT   QUERY.CFLINKS.G         NO_AUDIT
QUERY.CHANNEL.A         NO_AUDIT   QUERY.CHANNEL.C         NO_AUDIT
QUERY.CHANNEL.E         NO_AUDIT   QUERY.CHPID             NO_AUDIT
QUERY.CHPIDS.B          NO_AUDIT   QUERY.CHPIDS.E          NO_AUDIT
QUERY.CHPIDV            NO_AUDIT   QUERY.CMDLIMIT.A        NO_AUDIT
QUERY.CMDLIMIT.B        NO_AUDIT   QUERY.COLLECT           NO_AUDIT
QUERY.COMMANDS          NO_AUDIT   QUERY.CONCOPY           NO_AUDIT
QUERY.CONFIGMODE.B      NO_AUDIT   QUERY.CONFIGMODE.E      NO_AUDIT
QUERY.CONTROLLER        NO_AUDIT   QUERY.CONV              NO_AUDIT
QUERY.CPASSIST.A        NO_AUDIT   QUERY.CPASSIST.C        NO_AUDIT
QUERY.CPASSIST.E        NO_AUDIT   QUERY.CPCHECKING.A      NO_AUDIT
QUERY.CPCHECKING.C      NO_AUDIT   QUERY.CPCHECKING.E      NO_AUDIT
QUERY.CPCMDS.A          NO_AUDIT   QUERY.CPCMDS.C          NO_AUDIT
QUERY.CPCMDS.E          NO_AUDIT   QUERY.CPDISKS           NO_AUDIT
QUERY.CPLANGUAGE        NO_AUDIT   QUERY.CPLANGLIST        NO_AUDIT
QUERY.CPLEVEL           NO_AUDIT   QUERY.CPLOAD.A          NO_AUDIT
QUERY.CPLOAD.B          NO_AUDIT   QUERY.CPLOAD.E          NO_AUDIT
QUERY.CPOWNED           NO_AUDIT   QUERY.CPTRACE.A         NO_AUDIT
QUERY.CPTRACE.C         NO_AUDIT   QUERY.CPTRACE.E         NO_AUDIT
QUERY.CPTRAP            NO_AUDIT   QUERY.CPUAFFINITY       NO_AUDIT
QUERY.CPUID             NO_AUDIT   QUERY.CPXLOAD.A         NO_AUDIT
QUERY.CPXLOAD.C         NO_AUDIT   QUERY.CPXLOAD.E         NO_AUDIT
QUERY.CRYPTO.A          NO_AUDIT   QUERY.CRYPTO.B          NO_AUDIT
QUERY.CRYPTO.C          NO_AUDIT   QUERY.CRYPTO.E          NO_AUDIT
QUERY.CTCA              NO_AUDIT   QUERY.CU                NO_AUDIT
QUERY.DASD              NO_AUDIT   QUERY.DASDFW            NO_AUDIT
QUERY.DATEFORMAT        NO_AUDIT   QUERY.DIAGNOSE.A        NO_AUDIT
QUERY.DIAGNOSE.C        NO_AUDIT   QUERY.DIAGNOSE.E        NO_AUDIT
QUERY.DUPLEX            NO_AUDIT   QUERY.DISPLAY           NO_AUDIT
QUERY.DUMP              NO_AUDIT   QUERY.DUMPDEV           NO_AUDIT
QUERY.DYNAMIC_IO.B      NO_AUDIT   QUERY.DYNAMIC_IO.E      NO_AUDIT
QUERY.D8ONECMD.A        NO_AUDIT   QUERY.D8ONECMD.C        NO_AUDIT
QUERY.D8ONECMD.E        NO_AUDIT   QUERY.D8ONECMD.G        NO_AUDIT
QUERY.EDEVICE           NO_AUDIT   QUERY.EQID              NO_AUDIT
QUERY.EXITS.A           NO_AUDIT   QUERY.EXITS.C           NO_AUDIT
QUERY.EXITS.E           NO_AUDIT   QUERY.FCP               NO_AUDIT
QUERY.FENCES            NO_AUDIT   QUERY.FILES.D           NO_AUDIT
QUERY.FILES.G           NO_AUDIT   QUERY.FLASHCOPY         NO_AUDIT
QUERY.FRAMES.A          NO_AUDIT   QUERY.FRAMES.B          NO_AUDIT
QUERY.FRAMES.E          NO_AUDIT   QUERY.GATEWAY           NO_AUDIT
QUERY.GRAF              NO_AUDIT   QUERY.HCD               NO_AUDIT
QUERY.HOLD.B            NO_AUDIT   QUERY.HOLD.D            NO_AUDIT
QUERY.HOTIO             NO_AUDIT   QUERY.HYPERSWAP         NO_AUDIT
QUERY.ICLNAME.A         NO_AUDIT   QUERY.ICLNAME.C         NO_AUDIT
QUERY.ICLNAME.E         NO_AUDIT   QUERY.IMG.A             NO_AUDIT
QUERY.IMG.B             NO_AUDIT   QUERY.IMG.C             NO_AUDIT
QUERY.IMG.D             NO_AUDIT   QUERY.IMG.E             NO_AUDIT
QUERY.IOASSIST          NO_AUDIT   QUERY.IOPRIORITY.A      NO_AUDIT
QUERY.IOPRIORITY.E      NO_AUDIT   QUERY.IPLPARMS          NO_AUDIT
QUERY.ISFC              NO_AUDIT   QUERY.ISLINK            NO_AUDIT
QUERY.IUCV.B            NO_AUDIT   QUERY.IUCV.G            NO_AUDIT
QUERY.JOURNAL.A         NO_AUDIT   QUERY.JOURNAL.E         NO_AUDIT
QUERY.KEYALIAS          NO_AUDIT   QUERY.LDEVS.B           NO_AUDIT
QUERY.LDEVS.G           NO_AUDIT   QUERY.LINES             NO_AUDIT
QUERY.LINKS             NO_AUDIT   QUERY.LKFAC            NO_AUDIT
QUERY.LKFACR            NO_AUDIT   QUERY.LOADDEV          NO_AUDIT
QUERY.LOGMSG.A          NO_AUDIT   QUERY.LOGMSG.B          NO_AUDIT
QUERY.LOGMSG.C          NO_AUDIT   QUERY.LOGMSG.D          NO_AUDIT
QUERY.LOGMSG.E          NO_AUDIT   QUERY.LOGMSG.F          NO_AUDIT
QUERY.LOGMSG.G          NO_AUDIT   QUERY.LAN.B             NO_AUDIT
QUERY.LAN.G             NO_AUDIT   QUERY.LPARS            NO_AUDIT
QUERY.LSYSTEM           NO_AUDIT   QUERY.MAXLDEV          NO_AUDIT
QUERY.MAXSPOOL.D        NO_AUDIT   QUERY.MAXSPOOL.G        NO_AUDIT
QUERY.MAXUSERS          NO_AUDIT   QUERY.MDCACHE.B         NO_AUDIT
QUERY.MDCACHE.G         NO_AUDIT   QUERY.MDISK            NO_AUDIT
QUERY.MEMASSIST.B       NO_AUDIT   QUERY.MEMASSIST.G       NO_AUDIT
QUERY.MITIME.A          NO_AUDIT   QUERY.MITIME.B          NO_AUDIT
QUERY.MONDATA           NO_AUDIT   QUERY.MONITOR.A         NO_AUDIT
QUERY.MONITOR.E         NO_AUDIT   QUERY.MSS               NO_AUDIT
```

```
QUERY.NAMES.A               NO_AUDIT   QUERY.NAMES.B               NO_AUDIT
QUERY.NAMES.C               NO_AUDIT   QUERY.NAMES.D               NO_AUDIT
QUERY.NAMES.E               NO_AUDIT   QUERY.NAMES.F               NO_AUDIT
QUERY.NAMES.G               NO_AUDIT   QUERY.NEW_DEVICES           NO_AUDIT
QUERY.NIC                   NO_AUDIT   QUERY.NLS                   NO_AUDIT
QUERY.NSS                   NO_AUDIT   QUERY.NVS                   NO_AUDIT
QUERY.OBSERVER.A            NO_AUDIT   QUERY.OBSERVER.B            NO_AUDIT
QUERY.OBSERVER.C            NO_AUDIT   QUERY.OBSERVER.G            NO_AUDIT
QUERY.OSA                   NO_AUDIT   QUERY.PAGING.A              NO_AUDIT
QUERY.PAGING.C              NO_AUDIT   QUERY.PAGING.E              NO_AUDIT
QUERY.PASSWORD              NO_AUDIT   QUERY.PATHS.B               NO_AUDIT
QUERY.PATHS.E               NO_AUDIT   QUERY.PAV                   NO_AUDIT
QUERY.PENDING               NO_AUDIT   QUERY.PINNED                NO_AUDIT
QUERY.PF                    NO_AUDIT   QUERY.PORT                  NO_AUDIT
QUERY.PRINTER.D             NO_AUDIT   QUERY.PRINTER.G             NO_AUDIT
QUERY.PRIORITY.A            NO_AUDIT   QUERY.PRIORITY.B            NO_AUDIT
QUERY.PRIORITY.E            NO_AUDIT   QUERY.PRIORITY.F            NO_AUDIT
QUERY.PRIVCLASS.C           NO_AUDIT   QUERY.PRIVCLASS.E           NO_AUDIT
QUERY.PRIVCLASS.ANY         NO_AUDIT   QUERY.PROCESSORS.A          NO_AUDIT
QUERY.PROCESSORS.B          NO_AUDIT   QUERY.PROCESSORS.C          NO_AUDIT
QUERY.PROCESSORS.E          NO_AUDIT   QUERY.PRODUCT.C             NO_AUDIT
QUERY.PRODUCT.E             NO_AUDIT   QUERY.PROMPT                NO_AUDIT
QUERY.PSWTRANS              NO_AUDIT   QUERY.PUNCH.D               NO_AUDIT
QUERY.PUNCH.G               NO_AUDIT   QUERY.PVMSG                 NO_AUDIT
QUERY.QIOASSIST.B           NO_AUDIT   QUERY.QIOASSIST.G           NO_AUDIT
QUERY.QDROP.A               NO_AUDIT   QUERY.QDROP.B               NO_AUDIT
QUERY.QDROP.E               NO_AUDIT   QUERY.QDROP.F               NO_AUDIT
QUERY.QUICKDSP.A            NO_AUDIT   QUERY.QUICKDSP.E            NO_AUDIT
QUERY.READER.D              NO_AUDIT   QUERY.READER.G              NO_AUDIT
QUERY.RECORDING.A           NO_AUDIT   QUERY.RECORDING.B           NO_AUDIT
QUERY.RECORDING.C           NO_AUDIT   QUERY.RECORDING.E           NO_AUDIT
QUERY.RECORDING.F           NO_AUDIT   QUERY.REORDER.B             NO_AUDIT
QUERY.REORDER.E             NO_AUDIT   QUERY.RELODOMAIN.A          NO_AUDIT
QUERY.RELODOMAIN.B          NO_AUDIT   QUERY.RELODOMAIN.C          NO_AUDIT
QUERY.RELODOMAIN.E          NO_AUDIT   QUERY.RESERVED.A            NO_AUDIT
QUERY.RESERVED.E            NO_AUDIT   QUERY.RESOURCE              NO_AUDIT
QUERY.RETRIEVE              NO_AUDIT   QUERY.RSAW                  NO_AUDIT
QUERY.SASSIST.A             NO_AUDIT   QUERY.SASSIST.C             NO_AUDIT
QUERY.SASSIST.E             NO_AUDIT   QUERY.SCMBKS.B              NO_AUDIT
QUERY.SCMBKS.E              NO_AUDIT   QUERY.SCMEASURE.B           NO_AUDIT
QUERY.SCMEASURE.E           NO_AUDIT   QUERY.SCREEN                NO_AUDIT
QUERY.SDF.A                 NO_AUDIT   QUERY.SDF.B                 NO_AUDIT
QUERY.SDF.C                 NO_AUDIT   QUERY.SDF.D                 NO_AUDIT
QUERY.SDF.E                 NO_AUDIT   QUERY.SDF.G                 NO_AUDIT
QUERY.SECUSER.A             NO_AUDIT   QUERY.SECUSER.B             NO_AUDIT
QUERY.SECUSER.C             NO_AUDIT   QUERY.SECUSER.G             NO_AUDIT
QUERY.SET                   NO_AUDIT   QUERY.SHARE.A               NO_AUDIT
QUERY.SHARE.E               NO_AUDIT   QUERY.SHUTDOWNTIME.A        NO_AUDIT
QUERY.SHUTDOWNTIME.C        NO_AUDIT   QUERY.SIGNAL                NO_AUDIT
QUERY.SIGNALS               NO_AUDIT   QUERY.SPACES.E              NO_AUDIT
QUERY.SPACES.G              NO_AUDIT   QUERY.SPMODE.A              NO_AUDIT
QUERY.SPMODE.C              NO_AUDIT   QUERY.SPMODE.E              NO_AUDIT
QUERY.SRM.A                 NO_AUDIT   QUERY.SRM.E                 NO_AUDIT
QUERY.SSI.B                 NO_AUDIT   QUERY.SSI.E                 NO_AUDIT
QUERY.STGEXEMPT.A           NO_AUDIT   QUERY.STGEXEMPT.B           NO_AUDIT
QUERY.STGEXEMPT.C           NO_AUDIT   QUERY.STGEXEMPT.E           NO_AUDIT
QUERY.STGEXEMPT.G           NO_AUDIT   QUERY.STGLIMIT.A            NO_AUDIT
QUERY.STGLIMIT.B            NO_AUDIT   QUERY.STGLIMIT.C            NO_AUDIT
QUERY.STGLIMIT.E            NO_AUDIT   QUERY.STORAGE.A             NO_AUDIT
QUERY.STORAGE.B             NO_AUDIT   QUERY.STORAGE.E             NO_AUDIT
QUERY.STP                   NO_AUDIT   QUERY.SUBSTITUTE            NO_AUDIT
QUERY.SWITCHES              NO_AUDIT   QUERY.SXSPAGES.A            NO_AUDIT
QUERY.SXSPAGES.B            NO_AUDIT   QUERY.SXSPAGES.E            NO_AUDIT
QUERY.SXSSTORAGE.A          NO_AUDIT   QUERY.SXSSTORAGE.B          NO_AUDIT
QUERY.SXSSTORAGE.E          NO_AUDIT   QUERY.SYSASCII              NO_AUDIT
QUERY.SYSOPER               NO_AUDIT   QUERY.SYSTEM                NO_AUDIT
QUERY.S370E.A               NO_AUDIT   QUERY.S370E.C               NO_AUDIT
QUERY.S370E.E               NO_AUDIT   QUERY.TAG                   NO_AUDIT
QUERY.TAPES                 NO_AUDIT   QUERY.TDISK                 NO_AUDIT
QUERY.TDISKCLR              NO_AUDIT   QUERY.TERMINAL              NO_AUDIT
QUERY.THROTTLE.B            NO_AUDIT   QUERY.THROTTLE.E            NO_AUDIT
QUERY.TIME                  NO_AUDIT   QUERY.TIMEZONES             NO_AUDIT
QUERY.TOKEN                 NO_AUDIT   QUERY.TRACE                 NO_AUDIT
QUERY.TRACEFRAMES.A         NO_AUDIT   QUERY.TRACEFRAMES.B         NO_AUDIT
QUERY.TRACEFRAMES.C         NO_AUDIT   QUERY.TRACEFRAMES.E         NO_AUDIT
QUERY.TRFILES.A             NO_AUDIT   QUERY.TRFILES.C             NO_AUDIT
QUERY.TRFILES.D             NO_AUDIT   QUERY.TRFILES.E             NO_AUDIT
QUERY.TRFILES.G             NO_AUDIT   QUERY.TRSAVE.A              NO_AUDIT
QUERY.TRSAVE.C              NO_AUDIT   QUERY.TRSAVE.E              NO_AUDIT
QUERY.TRSAVE.G              NO_AUDIT   QUERY.TRSOURCE.A            NO_AUDIT
QUERY.TRSOURCE.C            NO_AUDIT   QUERY.TRSOURCE.E            NO_AUDIT
QUERY.TRSOURCE.G            NO_AUDIT   QUERY.UCR.A                 NO_AUDIT
```

```
QUERY.UCR.B                NO_AUDIT   QUERY.UCR.C                NO_AUDIT
QUERY.UNDERSCORE           NO_AUDIT   QUERY.UNRESOLVED.A         NO_AUDIT
QUERY.UNRESOLVED.C         NO_AUDIT   QUERY.UNRESOLVED.E         NO_AUDIT
QUERY.UR                   NO_AUDIT   QUERY.USERID               NO_AUDIT
QUERY.USERS                NO_AUDIT   QUERY.VCONFIG              NO_AUDIT
QUERY.VDISK                NO_AUDIT   QUERY.VMDUMP               NO_AUDIT
QUERY.VMLAN                NO_AUDIT   QUERY.VMSAVE.A             NO_AUDIT
QUERY.VMSAVE.C             NO_AUDIT   QUERY.VMSAVE.E             NO_AUDIT
QUERY.VMRELOCATE.A         NO_AUDIT   QUERY.VMRELOCATE.B         NO_AUDIT
QUERY.VMRELOCATE.C         NO_AUDIT   QUERY.VMRELOCATE.E         NO_AUDIT
QUERY.VMSG                 NO_AUDIT   QUERY.VRFREE               NO_AUDIT
QUERY.VSWITCH.B            NO_AUDIT   QUERY.VSWITCH.G            NO_AUDIT
QUERY.VTOD.A               NO_AUDIT   QUERY.VTOD.B               NO_AUDIT
QUERY.VTOD.G               NO_AUDIT   QUERY.VR                   NO_AUDIT
QUERY.WRKALLEG             NO_AUDIT   QUERY.XSTORAGE.B           NO_AUDIT
QUERY.XSTORAGE.E           NO_AUDIT   QUERY.V.ALL                NO_AUDIT
QUERY.V.CHPID              NO_AUDIT   QUERY.V.CONSOLE            NO_AUDIT
QUERY.V.CPUS               NO_AUDIT   QUERY.V.CRYPTO             NO_AUDIT
QUERY.V.CTCA               NO_AUDIT   QUERY.V.DASD               NO_AUDIT
QUERY.V.DUPLEX             NO_AUDIT   QUERY.V.FCP                NO_AUDIT
QUERY.V.FLASHCOPY          NO_AUDIT   QUERY.V.GRAF               NO_AUDIT
QUERY.V.LINES              NO_AUDIT   QUERY.V.MSGDEVICES         NO_AUDIT
QUERY.V.MSGPROC            NO_AUDIT   QUERY.V.NIC                NO_AUDIT
QUERY.V.OSA                NO_AUDIT   QUERY.V.PAV                NO_AUDIT
QUERY.V.PRINTER            NO_AUDIT   QUERY.V.PUNCH              NO_AUDIT
QUERY.V.READER             NO_AUDIT   QUERY.V.STORAGE            NO_AUDIT
QUERY.V.SWITCHES           NO_AUDIT   QUERY.V.SYSASCII           NO_AUDIT
QUERY.V.TAPES              NO_AUDIT   QUERY.V.UR                 NO_AUDIT
QUERY.V.XSTORAGE           NO_AUDIT   QUERY.VIRTUAL.B            NO_AUDIT
QUERY.VIRTUAL.G            NO_AUDIT   SET.ABEND                  NO_AUDIT
SET.ACCOUNT                NO_AUDIT   SET.ACNT                   NO_AUDIT
SET.ADJUNCTS               NO_AUDIT   SET.AFFINITY               NO_AUDIT
SET.ASSIST                 NO_AUDIT   SET.AUTOPOLL               NO_AUDIT
SET.CACHE                  NO_AUDIT   SET.CACHEFW                NO_AUDIT
SET.CCWTRAN                NO_AUDIT   SET.CFLINK.A               NO_AUDIT
SET.CFLINK.B               NO_AUDIT   SET.CFLINK.G               NO_AUDIT
SET.CMDLIMIT               NO_AUDIT   SET.CONCEAL                NO_AUDIT
SET.CONFIGMODE             NO_AUDIT   SET.CPASSIST               NO_AUDIT
SET.CPCHECKING.A           NO_AUDIT   SET.CPCHECKING.C           NO_AUDIT
SET.CPCONIO                NO_AUDIT   SET.CPLANGUAGE.B           NO_AUDIT
SET.CPLANGUAGE.G           NO_AUDIT   SET.CPTRACE.A              NO_AUDIT
SET.CPTRACE.C              NO_AUDIT   SET.CPUAFFINITY            NO_AUDIT
SET.CU                     NO_AUDIT   SET.CPUID                  NO_AUDIT
SET.DASDFW                 NO_AUDIT   SET.DATEFORMAT.B           NO_AUDIT
SET.DATEFORMAT.G           NO_AUDIT   SET.DEVICES                NO_AUDIT
SET.DUMP                   NO_AUDIT   SET.DUMPDEV                NO_AUDIT
SET.DYNAMIC_IO             NO_AUDIT   SET.D8ONECMD.A             NO_AUDIT
SET.D8ONECMD.G             NO_AUDIT   SET.ECMODE                 NO_AUDIT
SET.EDEVICE                NO_AUDIT   SET.EMSG                   NO_AUDIT
SET.FAVORED                NO_AUDIT   SET.HOTIO                  NO_AUDIT
SET.IMSG                   NO_AUDIT   SET.IOASSIST.B             NO_AUDIT
SET.IOASSIST.G             NO_AUDIT   SET.IOCDS_ACTIVE           NO_AUDIT
SET.IOPRIORITY             NO_AUDIT   SET.IPLPARMS               NO_AUDIT
SET.ISAM                   NO_AUDIT   SET.JOURNAL                NO_AUDIT
SET.KEYALIAS               NO_AUDIT   SET.LAN.B                  NO_AUDIT
SET.LAN.G                  NO_AUDIT   SET.LINEDIT                NO_AUDIT
SET.LKFAC                  NO_AUDIT   SET.LKFACR                 NO_AUDIT
SET.LOADDEV                NO_AUDIT   SET.LOGMSG                 NO_AUDIT
SET.LSYSTEM                NO_AUDIT   SET.MACHINE                NO_AUDIT
SET.MAXLDEV                NO_AUDIT   SET.MAXUSERS               NO_AUDIT
SET.MDCACHE.B              NO_AUDIT   SET.MDCACHE.G              NO_AUDIT
SET.MEMASSIST.B            NO_AUDIT   SET.MEMASSIST.G            NO_AUDIT
SET.MSG                    NO_AUDIT   SET.MSGFACIL               NO_AUDIT
SET.MIH                    NO_AUDIT   SET.MINWS                  NO_AUDIT
SET.MITIME.A               NO_AUDIT   SET.MITIME.B               NO_AUDIT
SET.MODE.A                 NO_AUDIT   SET.MODE.F                 NO_AUDIT
SET.MONDATA                NO_AUDIT   SET.NEW_DEVICES            NO_AUDIT
SET.NIC.B                  NO_AUDIT   SET.NIC.G                  NO_AUDIT
SET.NOPDATA                NO_AUDIT   SET.NOTRANS                NO_AUDIT
SET.NVS                    NO_AUDIT   SET.OBSERVER.A             NO_AUDIT
SET.OBSERVER.C             NO_AUDIT   SET.OBSERVER.G             NO_AUDIT
SET.PAGEX                  NO_AUDIT   SET.PAGING                 NO_AUDIT
SET.PASSWORD               NO_AUDIT   SET.PF                     NO_AUDIT
SET.PORT                   NO_AUDIT   SET.PRIORITY.A             NO_AUDIT
SET.PRIORITY.B             NO_AUDIT   SET.PRIORITY.E             NO_AUDIT
SET.PRIORITY.F             NO_AUDIT   SET.PRIVCLASS.C            NO_AUDIT
SET.PRIVCLASS.ANY          NO_AUDIT   SET.PRODUCT.C              NO_AUDIT
SET.PRODUCT.E              NO_AUDIT   SET.PROMPT                 NO_AUDIT
SET.PSWTRANS               NO_AUDIT   SET.QIOASSIST.B            NO_AUDIT
SET.QIOASSIST.G            NO_AUDIT   SET.QUICKDSP               NO_AUDIT
SET.QDROP.A                NO_AUDIT   SET.QDROP.B                NO_AUDIT
SET.QDROP.E                NO_AUDIT   SET.QDROP.F                NO_AUDIT
```

SET.RECORD	NO_AUDIT	SET.RDEVICE	NO_AUDIT
SET.REORDER	NO_AUDIT	SET.RESERVED	NO_AUDIT
SET.RETRIEVE.C	NO_AUDIT	SET.RETRIEVE.E	NO_AUDIT
SET.RETRIEVE.G	NO_AUDIT	SET.RUN	NO_AUDIT
SET.SASSIST	NO_AUDIT	SET.SCMEASURE.B	NO_AUDIT
SET.SCMEASURE.E	NO_AUDIT	SET.SECUSER.A	NO_AUDIT
SET.SECUSER.C	NO_AUDIT	SET.SECUSER.G	NO_AUDIT
SET.SHARE	NO_AUDIT	SET.SHARED	NO_AUDIT
SET.SHUTSIGNAL	NO_AUDIT	SET.SHUTDOWNTIME.A	NO_AUDIT
SET.SHUTDOWNTIME.C	NO_AUDIT	SET.SIGNAL.A	NO_AUDIT
SET.SIGNAL.C	NO_AUDIT	SET.SMSG	NO_AUDIT
SET.SRM	NO_AUDIT	SET.SSI	NO_AUDIT
SET.STBYPASS	NO_AUDIT	SET.STGEXEMPT.A	NO_AUDIT
SET.STGEXEMPT.B	NO_AUDIT	SET.STGEXEMPT.C	NO_AUDIT
SET.STGLIMIT.A	NO_AUDIT	SET.STGLIMIT.B	NO_AUDIT
SET.STGLIMIT.C	NO_AUDIT	SET.STMULTI	NO_AUDIT
SET.STORAGE	NO_AUDIT	SET.SVCACCL	NO_AUDIT
SET.SVC76	NO_AUDIT	SET.SYSOPER	NO_AUDIT
SET.S370E.A	NO_AUDIT	SET.S370E.G	NO_AUDIT
SET.TAPE	NO_AUDIT	SET.THROTTLE	NO_AUDIT
SET.TIMEBOMB	NO_AUDIT	SET.TIMER	NO_AUDIT
SET.TIMEZONE	NO_AUDIT	SET.TOKEN.B	NO_AUDIT
SET.TOKEN.E	NO_AUDIT	SET.TRACEFRAMES	NO_AUDIT
SET.UNDERSCORE	NO_AUDIT	SET.VCONFIG	NO_AUDIT
SET.VDISK	NO_AUDIT	SET.VMCONIO	NO_AUDIT
SET.VMLAN	NO_AUDIT	SET.VMRELOCATE	NO_AUDIT
SET.VMSAVE.A	NO_AUDIT	SET.VMSAVE.G	NO_AUDIT
SET.VSWITCH	NO_AUDIT	SET.VTOD.A	NO_AUDIT
SET.VTOD.B	NO_AUDIT	SET.VTOD.G	NO_AUDIT
SET.WNG	NO_AUDIT	SET.WRKALLEG	NO_AUDIT
SET.370ACCOM	NO_AUDIT	SET.370E	NO_AUDIT
DIAG000	NO_AUDIT	DIAG004	NO_AUDIT
DIAG008	NO_AUDIT	DIAG00C	NO_AUDIT
DIAG010	NO_AUDIT	DIAG014	NO_AUDIT
DIAG018	NO_AUDIT	DIAG020	NO_AUDIT
DIAG024	NO_AUDIT	DIAG028	NO_AUDIT
DIAG034	NO_AUDIT	DIAG03C	NO_AUDIT
DIAG040	NO_AUDIT	DIAG044	NO_AUDIT
DIAG048	NO_AUDIT	DIAG04C	NO_AUDIT
DIAG054	NO_AUDIT	DIAG058	NO_AUDIT
DIAG05C	NO_AUDIT	DIAG060	NO_AUDIT
DIAG064	NO_AUDIT	DIAG068	NO_AUDIT
DIAG070	NO_AUDIT	DIAG074	NO_AUDIT
DIAG07C	NO_AUDIT	DIAG084	NO_AUDIT
DIAG088	NO_AUDIT	DIAG08C	NO_AUDIT
DIAG090	NO_AUDIT	DIAG094	NO_AUDIT
DIAG098	NO_AUDIT	DIAG09C	NO_AUDIT
DIAG0A0	NO_AUDIT	DIAG0A4	NO_AUDIT
DIAG0A8	NO_AUDIT	DIAG0B0	NO_AUDIT
DIAG0B4	NO_AUDIT	DIAG0B8	NO_AUDIT
DIAG0BC	NO_AUDIT	DIAG0C4	NO_AUDIT
DIAG0C8	NO_AUDIT	DIAG0CC	NO_AUDIT
DIAG0D0	NO_AUDIT	DIAG0D4	NO_AUDIT
DIAG0D8	NO_AUDIT	DIAG0DC	NO_AUDIT
DIAG0E0	NO_AUDIT	DIAG0E4	NO_AUDIT
DIAG0EC	NO_AUDIT	DIAG0F0	NO_AUDIT
DIAG0F8	NO_AUDIT	DIAG204	NO_AUDIT
DIAG210	NO_AUDIT	DIAG214	NO_AUDIT
DIAG218	NO_AUDIT	DIAG220	NO_AUDIT
DIAG224	NO_AUDIT	DIAG238	NO_AUDIT
DIAG23C	NO_AUDIT	DIAG240	NO_AUDIT
DIAG244	NO_AUDIT	DIAG248	NO_AUDIT
DIAG250	NO_AUDIT	DIAG254	NO_AUDIT
DIAG258	NO_AUDIT	DIAG25C	NO_AUDIT
DIAG260	NO_AUDIT	DIAG264	NO_AUDIT
DIAG268	NO_AUDIT	DIAG26C	NO_AUDIT
DIAG270	NO_AUDIT	DIAG274	NO_AUDIT
DIAG278	NO_AUDIT	DIAG27C	NO_AUDIT
DIAG280	NO_AUDIT	DIAG288	NO_AUDIT
DIAG290	NO_AUDIT	DIAG29C	NO_AUDIT
DIAG2A0	NO_AUDIT	DIAG2A4	NO_AUDIT
DIAG2A8	NO_AUDIT	DIAG2AC	NO_AUDIT
DIAG2C0	NO_AUDIT	DIAG2C4	NO_AUDIT
DIAG2CC	NO_AUDIT	DIAG2E0	NO_AUDIT
DIAG2FC	NO_AUDIT	DIAG308	NO_AUDIT
IUCVCON	NO_AUDIT	IUCVSEV	NO_AUDIT
APPCCON	NO_AUDIT	APPCPWVL	NO_AUDIT
APPCSEV	NO_AUDIT	SPF_CREATE	NO_AUDIT
SPF_DELETE	NO_AUDIT	SPF_OPEN	NO_AUDIT
SDF_CREATE	NO_AUDIT	SDF_DELETE	NO_AUDIT
SDF_OPEN	NO_AUDIT	UTLPRINT	NO_AUDIT
MDISK	NO_AUDIT	MAINTCCW	NO_AUDIT

```
RSTDSEG                      NO_AUDIT   SNIFFER_MODE                NO_AUDIT
DIRECTRY_CMD                 NO_AUDIT   SCIF                        NO_AUDIT
RDEVCTRL                     NO_AUDIT
RPISET126I SETEVENT COMPLETED SUCCESSFULLY.
```

SETRACF (Deactivate/Reactivate RACF on z/VM)

System environment

This command applies to z/VM systems only.

SETRACF is a CMS command, not a RACF command. As a result, you cannot issue SETRACF using RAC or during a RACF command session.

You can issue the SETRACF command only from a RACF service machine. The RACF service machine can, however run disconnected, thereby allowing a secondary console to issue this command.

By default, RACF sets up the OPERATOR as the secondary console for the RACF service machine; the OPERATOR can issue the command to deactivate RACF. For example,

```
SEND RACFVM SETRACF INACTIVE
```

If you issue SETRACF for any RACF service machine in a multiple service machine environment, it will apply to all service machines.

Purpose

Use the SETRACF command to temporarily deactivate RACF.

Caution: Use care when issuing SETRACF to deactivate RACF. When you deactivate RACF, access control reverts to z/VM. z/VM uses the information in the CP directory to control a user's access to the system (using the user's password) and to minidisks (using z/VM links). The information in the CP directory is probably not current with the equivalent information in the RACF database. In particular, the CP directory does not support password phrases. If you have any "phrase-only" users defined, they will not be able to LOGON.

For example, if your installation changes a user's access authority to a minidisk from CONTROL to READ in the RACF database, this change is not reflected automatically in the CP directory.

If you find it necessary to deactivate RACF, you should not allow general users to log on to the system while RACF is inactive.

Related Commands

To work with the RACF databases, use the RVARY command as described in “RVARY (Change Status of RACF Database)” on page 261.

Authorization Required

When you issue SETRACF to deactivate RACF, you require information from the primary system operator. The system notifies the operator and asks the operator if RACF can be deactivated. The operator must approve before RACF can be deactivated. If CP is reinitialized, RACF deactivation does not remain in effect.

Syntax

The complete syntax of the command is:

SETRACF	ACTIVE | INACTIVE

Parameters

ACTIVE | INACTIVE

ACTIVE
specifies that you want to reactivate RACF.

INACTIVE
specifies that you want to temporarily deactivate RACF.

SETROPTS (Set RACF Options)

System environment

This command applies to both z/OS and z/VM systems.

Purpose

Use the SETROPTS command to set system-wide RACF options related to resource protection dynamically. Specifically, you can use SETROPTS to do the following on both z/OS and z/VM systems:

- Gather and display RACF statistics
- Protect terminals
- Log RACF events
- Permit list-of-groups access checking
- Display options currently in effect
- Enable or disable the generic profile checking facility on a class-by-class basis or for all classes system-wide
- Control change interval for user passwords and password phrases
- Establish password syntax rules
- Activate checking for previous passwords and password phrases
- Control mixed-case passwords.
- Limit unsuccessful attempts to access the system using incorrect passwords and password phrases.
- Activate auditing for access attempts by class
- Activate auditing for security labels
- Require that all work entering the system, including users logging on and batch jobs, have a security label assigned
- Enable or disable the global access checking facility
- Refresh in-storage profile lists and global access checking tables
- Set the password the operator must supply in order for RACF to complete an RVARY command that changes RACF status or changes the RACF databases
- Enable or disable the sharing, in common storage, of discrete and generic profiles for general resource classes
- Activate or deactivate auditing of access attempts to RACF-protected resources based on installation-defined security levels

In addition, you can use the SETROPTS command to do the following on z/OS systems only:

- Control the automatic data set protection (ADSP) attribute for users
- Activate profile modeling for GDG, group, and user data sets
- Activate protection for data sets with single-level names
- Control logging of real data set names
- Control the job entry subsystem options
- Activate tape data set protection
- Control whether RACF is to allow users to create or access data sets that do not have RACF protection
- Activate and control the scope of erase-on-scratch processing
- Activate program control, which includes both access control to load modules and program access to data

- Prevent users from accessing uncataloged permanent data sets
- Establish a system-wide VTAM* session interval
- Set an installation-wide default for the RACF security retention period for tape data sets
- Activate enhanced generic naming for data sets and entries in the global access checking table
- Set installation defaults for primary and secondary national languages.
- Activate auditing for APPC transactions

If you specify the AUDIT operand, RACF logs all uses of the RACDEF SVC and all changes made to profiles by RACF commands. Following are the classes that can be specified in the AUDIT operand and the commands and SVCs that will be logged for each class:

FILE	DIRECTRY	USER	GROUP	DATASET	CDT Entries
ADDFILE	ADDDIR	ADDUSER	ADDGROUP	ADDSD	PERMIT
ALTFILE	ALTDIR	ALTUSER	ALTGROUP	ALTDSD	RACDEF SVC
DELFILE	DELDIR	CONNECT	CONNECT	DELDSD	RALTER
PERMFILE	PERMDIR	DELUSER	DELGROUP	PERMIT	RDEFINE
RDEFINE	RDEFINE	PASSWORD	REMOVE	RACDEF SVC	RDELETE
RALTER	RALTER	REMOVE			
RDELETE	RDELETE				
PERMIT	PERMIT				
RACDEF SVC	RACDEF SVC				

Most RACF functions do not require special versions or releases of the operating system or operating system components. Some, however, do require that your system be at a certain level. If you are unsure about whether or not a particular RACF function is available with your system, see the matrix of new functions at the beginning of this book.

Note:

1. The options you specify on SETROPTS are common on systems that share the RACF database. All the systems involved must have the required levels of software. If you activate the SECLABEL and ML options on one system, they will be activated on all systems.
2. If you issue the SETROPTS command with any operand that changes the RACF database or issue the SETROPTS REFRESH command, the command is automatically propagated to all RACF servers that run on the same z/VM system, and to other systems in the same SSI cluster as the issuing system. Only the SETROPTS LIST command is not propagated.

   On a system outside an SSI cluster, the action is not propagated to other systems that share the RACF database. You must issue the SETROPTS command separately for each system or restart the RACF servers on the other system or IPL the other system.
3. RACF interprets dates with 2 digit years in the following way, YY represents the 2 digit year.

```
IF 70 < YY <= 99 THEN
   The date is interpreted as 19YY
IF 00 <= YY <= 70 THEN
   The date is interpreted as 20YY
```

Authorization Required

Most SETROPTS command functions require you to have the SPECIAL or AUDITOR attribute.

If you have the SPECIAL attribute, you can use all of the operands except those listed below, which require the AUDITOR attribute:

- APPLAUDIT | NOAPPLAUDIT
- AUDIT | NOAUDIT
- CMDVIOL | NOCMDVIOL
- LOGOPTIONS
- OPERAUDIT | NOOPERAUDIT
- SAUDIT | NOSAUDIT
- SECLABELAUDIT | NOSECLABELAUDIT
- SECLEVELAUDIT | NOSECLEVELAUDIT

If you have the SPECIAL, AUDITOR, or ROAUDIT attribute, you can use the LIST operand.

In some situations, you can use SETROPTS even if you do not have the SPECIAL, AUDITOR, or ROAUDIT attribute. These situations are:

- You can specify the LIST operand if you have the group-SPECIAL or group-AUDITOR attribute in the current connect group or if GRPLIST is active in any group that you are connected to.
- You can specify REFRESH together with GENERIC if you have the group-SPECIAL, AUDITOR, group-AUDITOR, OPERATIONS, or group-OPERATIONS attribute, or CLAUTH authority for the classes specified.
- You can specify REFRESH together with GLOBAL if you have the OPERATIONS attribute or CLAUTH authority for the classes specified.
- You can specify REFRESH together with RACLIST if you have CLAUTH authority to the specified class.
- On z/OS, you can specify REFRESH together with WHEN(PROGRAM) if you have CLAUTH authority for the program class.

Note: The syntax diagram does not indicate the defaults that are in effect when you first initialize RACF. (You can find these defaults in the description of each operand.) As you establish the system-wide defaults your installation needs, you might find it useful to mark the syntax diagram to reflect your choices.

Syntax

The full command name is SETROPTS. The minimum command abbreviation is SETR.

The following operands are valid in all environments:

```
[ ADDCREATOR | NOADDCREATOR ]
[ {AUDIT | NOAUDIT} ({class-name ... | *}) ]
[ {CLASSACT | NOCLASSACT} ( {class-name... | *} ) ]
[ CMDVIOL | NOCMDVIOL ]
[ COMPATMODE | NOCOMPATMODE ]
[ EGN | NOEGN ]
[ {GENCMD | NOGENCMD} ( {class-name... | *} ) ]
[ {GENERIC | NOGENERIC} ( {class-name... | *} ) ]
[ GENERICOWNER | NOGENERICOWNER ]
[ {GENLIST | NOGENLIST} (class-name ...) ]
[ {GLOBAL | NOGLOBAL} ( {class-name ... | *} ) ]
[ GRPLIST | NOGRPLIST ]
[ INACTIVE(unused-userid-interval) | NOINACTIVE ]
[ INITSTATS | NOINITSTATS ]
[ LIST ]
[ LOGOPTIONS(
  {ALWAYS(class-name, ...), ...
  | NEVER(class-name, ...), ...
```

```
  | SUCCESSES(class-name, ...), ...
  | FAILURES(class-name, ...), ...
  | DEFAULT( {class-name, ... | *} ) }
  ) ]
[ MLACTIVE [( FAILURES | WARNING )] | NOMLACTIVE ]
[ MLQUIET | NOMLQUIET ]
[ MLS [( FAILURES | WARNING ) ] | NOMLS ]
[ MLSTABLE | NOMLSTABLE ]
[ OPERAUDIT | NOOPERAUDIT ]
[ PASSWORD(
  [ ALGORITHM(KDFAES) | NOALGORITHM ]
  [ HISTORY(number-previous-values) | NOHISTORY ]
  [ INTERVAL(maximum-change-interval) ]
  [ MINCHANGE(minimum-change-interval) ]
  [ MIXEDCASE | NOMIXEDCASE ]
  [ REVOKE(number-invalid-attempts) | NOREVOKE    ]
  [ {RULEn(LENGTH(m1:m2) content-keyword (position))
     | NORULEn
     | NORULES} ]
  [ SPECIALCHARS | NOSPECIALCHARS ]
  [ WARNING(days-before-expiration) | NOWARNING ]
  ) ]
[ {RACLIST | NORACLIST} (class-name ...) ]
[ REFRESH ]
[ RVARYPW( [SWITCH(switch-pw)] [STATUS(status-pw)] ) ]
[ SAUDIT | NOSAUDIT ]
[ SECLABELAUDIT(seclabel-name ...) | NOSECLABELAUDIT ]
[ SECLABELCONTROL(seclabel-name ...)
  | NOSECLABELCONTROL ]
[ SECLEVELAUDIT (security-level) | NOSECLEVELAUDIT ]
[ SESSIONINTERVAL(n) | NOSESSIONINTERVAL]
[ {STATISTICS | NOSTATISTICS} ({class-name... | *}) ]
[ TERMINAL( NONE | READ ) ]
```

The following operands are valid only in z/OS systems:

```
[ ADSP | NOADSP ]
[ APPLAUDIT | NOAPPLAUDIT ]
[ CATDSNS ( FAILURES | WARNING ) | NOCATDSNS ]
[ ERASE [(
  { ALL
  | SECLEVEL(seclevel-name)
  | NOSECLEVEL}
  )]
| NOERASE ]
[ JES (
  [ BATCHALLRACF | NOBATCHALLRACF ]
  [ EARLYVERIFY | NOEARLYVERIFY ]
  [ XBMALLRACF | NOXBMALLRACF ]
  [ NJEUSERID(userid) ]
  [ UNDEFINEDUSER(userid) ]
  ) ]
[ LANGUAGE(
  [ PRIMARY(language)   ]
  [ SECONDARY(language) ]
  ) ]
[ MODEL(
```

```
  [ GDG   | NOGDG   ]
  [ GROUP | NOGROUP ]
  [ USER  | NOUSER  ])
| NOMODEL ]
[ PREFIX(prefix) | NOPREFIX ]
[ PROTECTALL [( FAILURES | WARNING )] | NOPROTECTALL ]
[ REALDSN | NOREALDSN ]
[ RETPD(nnnnn) ]
[ TAPEDSN | NOTAPEDSN ]
[ {WHEN | NOWHEN} (PROGRAM) ]
```

Parameters

ADDCREATOR | NOADDCREATOR

ADDCREATOR

Specifies that if a user defines any new DATASET or general resource profile using ADDSD, RDEFINE, or RACROUTE REQUEST=DEFINE, the profile creator's user ID is placed on the profile access list with ALTER authority.

NOADDCREATOR

Specifies that if a user defines any new DATASET or general resource profile using ADDSD, RDEFINE or RACROUTE REQUEST=DEFINE, or creates discrete profile other than DATASET and TAPEVOL using RACROUTE REQUEST=DEFINE, RACF does not place the profile creator's user ID on the profile's access list. If the profile creator uses profile modeling, RACF copies the access list exactly. If the creator's user ID appears in the model's access list, RACF copies the authority to the new profile. For example, if the creator's user ID appears in the model's access list with READ, RACF copies that access authority to the new profile without changing it to ALTER.

An important exception for NOADDCREATOR occurs when the user creates a discrete DATASET or TAPEVOL profile using RACROUTE REQUEST=DEFINE. In this case, RACF ignores the NOADDCREATOR options and places the profile creator's user ID on the new profile's access list with ALTER authority. If the profile creator uses profile modeling to define a discrete DATASET or TAPEVOL and the creator's user ID appears in the model's access list, RACF creates the new profile with ALTER authority. This exception to NOADDCREATOR allows system components to allocate data sets and immediately access them without having an administrator manipulate the profile's access list in the interim.

Note: The initial setting of the ADDCREATOR/NOADDCREATOR keyword depends on whether your database is new or old. When IRRMIN00 is run with PARM=NEW, the initial setting is NOADDCREATOR. When IRRMIN00 is run with anything other than PARM=NEW, RACF retains the current value of ADDCREATOR/NOADDCREATOR. For compatibility and migration reasons, this value is set to ADDCREATOR if no prior specification of ADDCREATOR or NOADDCREATOR had occurred.

ADSP | NOADSP

Note: *These operands apply to z/OS systems only.*

ADSP

specifies that data sets created by users who have the automatic data set protection (ADSP) attribute will be RACF-protected automatically. ADSP is in effect when RACF is first installed.

Because ADSP forces the creation of a discrete profile for each data set created by users who have the ADSP attribute, you should normally specify NOADSP if you specify GENERIC.

NOADSP

cancels automatic RACF protection for users who have the ADSP attribute.

Because ADSP forces the creation of a discrete profile for each data set created by users who have the ADSP attribute, you should normally specify NOADSP if you specify GENERIC.

APPLAUDIT | NOAPPLAUDIT

Note: *These operands apply to z/OS systems only.*

APPLAUDIT
specifies that auditing of APPC transactions on your system be enabled. APPC transactions are audited when they receive authorization (start) or have authorization removed (end). You must request auditing for the appropriate APPL profile. Otherwise, turning APPLAUDIT on will not cause auditing of APPC transactions. See *z/VM: RACF Security Server Auditor's Guide* for more information on requesting auditing.

You must have the AUDITOR attribute to specify this option.

NOAPPLAUDIT
specifies that auditing of APPC transactions on your system (starting and ending) be disabled. You must have the AUDITOR attribute to specify this option.

AUDIT | NOAUDIT

AUDIT(*class-name ... | **)
specifies the names of the classes for which you want RACF to perform auditing. For the classes you specify, RACF logs all uses of the RACDEF SVC and all changes made to profiles by RACF commands. (RACF adds the classes you specify to those already specified for auditing.)

The valid class names are USER, GROUP, DATASET, and those defined in the class descriptor table (CDT). For a list of general resource classes supplied by IBM, see Appendix B, "IBM-Supplied Resource Classes that Apply to z/VM Systems," on page 349.

When the class specified is USER, RACF logs all password and password phrase changes made by RACROUTE REQUEST=VERIFY.

If you specify an asterisk (*), logging will occur for all classes.

You must have the AUDITOR attribute to enter the AUDIT operand.

Note: If you activate auditing for a class using SETROPTS AUDIT, RACF activates auditing for all classes in the class descriptor table (CDT) that have the same POSIT value as the class you specify. For example, the classes TIMS, GIMS, and AIMS all have a POSIT value of 4 in their respective CDT entries. If you activate auditing for any one of these classes, you will activate auditing for all of them.

For more information, see the description of the ICHERCDE macro in *z/VM: RACF Security Server Macros and Interfaces*.

NOAUDIT(*class-name ... | **)
specifies the names of the classes for which you no longer want RACF to perform auditing. For the classes you specify, RACF no longer logs all uses of the RACDEF SVC and all changes made to profiles by RACF commands. The valid class names are USER, GROUP, DATASET, and those classes defined in the class descriptor table (CDT). For a list of general resource classes supplied by IBM, see Appendix B, "IBM-Supplied Resource Classes that Apply to z/VM Systems," on page 349.

NOAUDIT(*) is in effect when RACF is first installed. If you specify an asterisk (*), logging will not occur for any of the classes.

You must have the AUDITOR attribute to enter the NOAUDIT operand.

Note: If you deactivate auditing for a class using SETROPTS NOAUDIT, RACF deactivates auditing for all classes in the CDT that have the same POSIT value as the class you specify. For example, the classes TIMS, GIMS, and AIMS all have a POSIT value of 4 in their respective CDT entries. If you deactivate auditing for any one of these classes, you will deactivate auditing for all of them.

For more information, see the description of the ICHERCDE macro in *z/VM: RACF Security Server Macros and Interfaces*.

CATDSNS | NOCATDSNS
Note: *These operands apply to z/OS systems only.*

CATDSNS (FAILURES | WARNING)
prevents users from accessing uncataloged, new (and not yet cataloged), or system temporary data sets.

The following exceptions apply:

1. The job that creates the data set may access it even if the data set is uncataloged. If the data set is still uncataloged when the job ends, it will be inaccessible thereafter.
2. Data sets with discrete profiles may be accessed—even if uncataloged—if allowed by the profile.
3. For data sets that have no discrete profile, if private catalogs for the job are in use, RACF checks the users authority to a resource named ICHUSERCAT in the FACILITY class. If the resource is protected and the user has access to it, processing continues with the next step. Otherwise, access to the data set will be denied.
4. For uncataloged data sets without discrete profiles, RACF constructs a resource name of ICHUNCAT.*dsname* (only the first 30 characters of the dsname is used). It checks the user's authority to this resource in the FACILITY class. If the resource is protected by a FACILITY class profile, and the user has access to it, the access is allowed.
5. If the user has the SPECIAL attribute, the access is allowed even if the data set is uncataloged, but a warning message and SMF record is created.

CATDSNS has a negative impact on RACF and system performance because RACF verifies that data sets are cataloged before it allows them to be opened.

FAILURES
specifies that RACF is to reject any request to access a data set that is not cataloged.

FAILURES is the default.

If CATDSNS(FAILURES) is in effect and a privileged started task or a user with the SPECIAL attribute requests access of an uncataloged data set, RACF accepts the request and issues a warning message.

WARNING
specifies that the access will be allowed even if the data set is uncataloged. However, a warning message and SMF record will be created.

NOCATDSNS
specifies that datasets that are not cataloged can be accessed by users.

NOCATDSNS is in effect when RACF is first installed.

CLASSACT | NOCLASSACT

CLASSACT(*class-name* ...|*)
specifies those classes defined by entries in the class descriptor table for which RACF protection is to be in effect.

ATTENTION: Do not specify an asterisk (*), unless you have defined profiles for *all* classes defined in the class descriptor table.

You should only activate the classes that are important to your installation, as some classes have a default return code of 8:

```
APPCSERV     JESINPUT    SECLABEL
APPCTP       JESJOBS     TEMPDSN
CONSOLE      JESSPOOL    WRITER
DIRAUTH      PSFMPL
```

These classes should only be activated after you have defined the necessary profiles to allow access to resources.

If you specify an asterisk (*), you activate RACF protection for all classes defined in the class descriptor table except for those classes with a default return code of 8.

For a list of general resource classes supplied by IBM, see Appendix B, "IBM-Supplied Resource Classes that Apply to z/VM Systems," on page 349.

Note:

1. If you activate a class using SETROPTS CLASSACT, RACF activates all classes in the class descriptor table (CDT) that have the same POSIT value as the class you specify. For example, the classes TIMS, GIMS, and AIMS all have a POSIT value of 4 in their respective CDT entries. If you activate any one of these classes, you will activate all of them.

   For more information, see the description of the ICHERCDE macro in *z/VM: RACF Security Server Macros and Interfaces*.
2. When the SETROPTS CLASSACT(SECLABEL) command is issued, z/VM does not call for MAC authorization *until* after one authorization or audit call is made to RACF. Once any call from z/VM to RACF has been made for a z/VM event, z/VM begins calling RACF for MAC authorization. In other words, z/VM is not notified when the SETROPTS CLASSACT(SECLABEL) command is issued. Instead z/VM is notified when z/VM calls RACF next.

   For more information see *z/VM: RACF Security Server Security Administrator's Guide*.
3. Before activating a class that has a default return code of 8 in the CDT (either explicitly or by means of a shared POSIT value), be sure you have defined the necessary profiles to allow your users to access resources in that class. For example, on z/OS, if you activate JESINPUT without defining profiles to allow access, no one will be able to submit batch jobs.
4. If you activate the TEMPDSN class, you must have DFP Release 3.1 (with PTF UY34317) or later installed.

NOCLASSACT(*class-name*...|*)
specifies those classes defined by entries in the CDT for which RACF protection is not to be in effect. If you specify an asterisk (*), you deactivate RACF protection for all classes defined in the CDT. For a list of general resource classes supplied by IBM, see Appendix B, "IBM-Supplied Resource Classes that Apply to z/VM Systems," on page 349.

NOCLASSACT is in effect when RACF is first installed.

Note: If you deactivate a class using SETROPTS NOCLASSACT, RACF deactivates all classes in the CDT that have the same POSIT value as the class you specify. For example, the classes TIMS, GIMS, and AIMS all have a POSIT value of 4 in their respective CDT entries. If you deactivate any one of these classes, you will deactivate all of them.

For more information, see the description of the ICHERCDE macro in *z/VM: RACF Security Server Macros and Interfaces*.

CMDVIOL | NOCMDVIOL
specify whether RACF is to log violations detected by RACF commands. You must have the AUDITOR attribute to specify these options.

CMDVIOL
specifies that RACF is to log violations detected by RACF commands (except LDIRECT, LFILE, LISTDSD, LISTGRP, LISTUSER, RLIST, and SEARCH) during RACF command processing. A violation may occur because a user is not authorized to modify a particular profile or is not authorized to enter a particular operand on a command. CMDVIOL is in effect when RACF is first installed.

NOCMDVIOL
specifies that RACF is not to log violations detected by RACF commands during RACF command processing (except RVARY and SETROPTS, which are always logged).

COMPATMODE | NOCOMPATMODE

COMPATMODE
allows users and jobs not using SECLABELs to be on a system enforcing SECLABELs. The ACEE's of the user IDs or jobs must have been created by a RACINIT macro that did not specify RACF Release 1.9 keywords.

NOCOMPATMODE
Users and jobs must be running with correct security labels to access data.

NOCOMPATMODE is in effect when RACF is first installed.

EGN | NOEGN
activate or deactivate enhanced generic naming (EGN).

EGN
activates EGN. When you activate this option, RACF allows you to specify the generic character ** (in addition to the generic characters * and %) when you define data set profile names and entries in the global access checking table.

Note:

1. EGN changes the meaning of the generic character *.
2. When you first activate enhanced generic naming, the RACF-protection provided by existing data set profiles and global access checking table remains the same.

For information on EGN and its effect on profile names, see the description of generic profiles in Appendix A, “Resource Profile Naming Considerations,” on page 335.

NOEGN
specifies deactivation of EGN. When you deactivate this option, RACF does not allow you to specify the generic character ** when you define data set names and entries in the global access checking table.

NOEGN is in effect when RACF is first installed.

> **Attention:** If you protect data sets with generic profiles while EGN is active and then deactivate this option, your resources may no longer be protected. Table 5 on page 338 and Table 6 on page 338 show examples of generic profiles created with enhanced generic naming active.
>
> Some of these profiles do not provide RACF protection when the option is deactivated. If a data set will be unprotected when EGN is deactivated, you can protect the data set with a discrete profile as described in Appendix A, “Resource Profile Naming Considerations,” on page 335 either before or after the option is deactivated, or with a generic profile after the option is deactivated.

ERASE | NOERASE
Note: *These operands apply to z/OS systems only.*

ERASE(*erase-indicator*)
specifies that data management is to physically erase the DASD data set extents at the time the DASD data set is deleted (scratched) or released for reuse. When RACF is running on a system that includes data management support for erase-on-scratch, the allocated extents of a scratched and erased data set are overwritten with binary zeros.

If you specify ERASE without any suboperands, whether a scratched data set is erased depends on the contents of the erase indicator in the data set profile. The ERASE suboperands allow you to override the erase indicator in the data set profile, to control the scope of erase-on-scratch on an installation level rather than leaving it to individual users.

The variable *erase-indicator* can be:

ALL
specifies that data management is to erase all scratched DASD data sets, including temporary data sets, regardless of the erase indicator, if any, in the data set profile.

SECLEVEL(*seclevel-name*)
specifies that data management is to erase all scratched DASD data sets that have a security level equal to or greater than the security level that you specify, where *seclevel-name* must be a member of the SECLEVEL profile in the SECDATA class.

Note: Scratched DASD datasets with a security level lower than the level you specify will not be erased, regardless of the erase indicators (if any) in the dataset profiles.

NOSECLEVEL
specifies that RACF is not to use the security level in the data set profile when it decides whether data management is to erase a scratched DASD data set.

Specifying ERASE(NOSECLEVEL) causes RACF to use the erase indicator in the data set profile to decide whether data management is to scratch the data set. NOSECLEVEL is the default if you do not specify *erase-indicator* when you specify ERASE.

NOERASE
specifies that erase-on-scratch processing is not in effect. NOERASE means that no DASD data sets are erased when deleted (scratched), even if the erase indicator in the data set profile is on.

NOERASE is in effect when RACF is first installed.

GENCMD | NOGENCMD

GENCMD(*class-name* ...|*)
activates generic profile command processing for the specified classes. Valid class names you can specify are DATASET and all class names defined in the class descriptor table (CDT) except grouping classes. If you specify an asterisk (*), you activate generic profile command processing for the DATASET class plus all the classes defined in the CDT except grouping classes. For a list of general resource classes supplied by IBM, see Appendix B, "IBM-Supplied Resource Classes that Apply to z/VM Systems," on page 349.

When GENCMD is in effect for a class, all the command processors can work on generic profiles, but the RACF SVC routines cannot perform generic profile checking. This operand allows the installation to temporarily disable generic profile checking (during maintenance, for example) and still use the RACF commands to maintain generic profiles.

Note: If you activate generic profile command processing for a class using SETROPTS GENCMD, RACF activates generic profile command processing for all classes in the CDT that have the same POSIT value as the class you specify, except grouping classes. For example, the resource classes TIMS and AIMS and the grouping class GIMS all have a POSIT value of 4 in their respective CDT entries. If you activate generic profile command processing for TIMS, you will also activate it for AIMS. However, you cannot activate this option for GIMS because GIMS is a grouping class.

For more information, see the description of the ICHERCDE macro in *z/VM: RACF Security Server Macros and Interfaces*.

NOGENCMD(*class-name* ...|*)
deactivates generic profile command processing for the specified classes. Valid class names you can specify are DATASET and all class names defined in the class descriptor table (CDT) except grouping classes. If you specify an asterisk (*), you deactivate generic profile command processing for the DATASET class plus all the classes in the CDT (excluding grouping classes). For a list of general resource classes defined in the IBM-supplied CDT, see Appendix B, "IBM-Supplied

Resource Classes that Apply to z/VM Systems," on page 349. NOGENCMD(*) is in effect when RACF is first installed.

If generic profile checking is active (GENERIC is in effect), RACF ignores this operand because GENERIC both includes and overrides generic profile command processing.

Note: If you deactivate generic profile command processing for a class using SETROPTS NOGENCMD, RACF deactivates generic profile command processing for all classes in the CDT that have the same POSIT value as the class you specify, except grouping classes. For example, the resource classes TIMS and AIMS and the grouping class GIMS all have a POSIT value of 4 in their respective CDT entries. If you deactivate generic profile command processing for TIMS, you will also deactivate it for AIMS. However, GIMS is unaffected because it is a grouping class.

For more information, see the description of the ICHERCDE macro in *z/VM: RACF Security Server Macros and Interfaces*.

GENERIC | NOGENERIC

GENERIC(*class-name* ...|*)
activates generic profile checking for the classes specified. Valid class names you can specify are DATASET and all class names defined in the class descriptor table (CDT) except grouping classes. If you specify an asterisk (*), you activate generic profile checking for the DATASET class plus all the classes in the CDT except grouping classes. For a list of general resource classes supplied by IBM, see Appendix B, "IBM-Supplied Resource Classes that Apply to z/VM Systems," on page 349.

Generic profile command processing is automatically activated for all classes for which generic profile checking is activated.

If you specify GENERIC with REFRESH, only those currently active and authorized classes are refreshed.

Note:

1. RACF does not automatically propagate the SETROPTS command to other non-cluster systems sharing the database for the combination of the GENERIC and REFRESH options. For this combination of options, the SETROPTS command must be issued to each system sharing the database. See Note "2" on page 289 for more information.
2. If you specify GENERIC, you should also specify NOADSP.
3. If you activate generic profile checking for a class using SETROPTS GENERIC, RACF activates generic profile checking for all classes in the CDT that have the same POSIT value as the class you specify, except grouping classes. For example, the resource classes TIMS and AIMS and the grouping class GIMS all have a POSIT value of 4 in their respective CDT entries. If you activate generic profile checking for TIMS, you will also activate it for AIMS. However, you cannot activate this option for GIMS because GIMS is a grouping class.

For more information, see the description of the ICHERCDE macro in *z/VM: RACF Security Server Macros and Interfaces*.

NOGENERIC(*class-name* ...|*)
deactivates the generic profile checking facility for the classes specified. Valid class names you can specify are DATASET and all class names defined in the CDT except grouping classes. If you specify an asterisk (*), you deactivate generic profile checking for the DATASET class plus all the classes in the CDT (excluding grouping classes). For a list of general resource classes defined in the IBM-supplied CDT, see Appendix B, "IBM-Supplied Resource Classes that Apply to z/VM Systems," on page 349. NOGENERIC (*) is in effect when RACF is first installed.

If you specify GENCMD with NOGENERIC, users can issue RACF commands to maintain generic profiles, but RACF does not use generic profile checking during authorization checking.

If you specify NOGENCMD with NOGENERIC, all generic profile command processing is deactivated.

Note: If you deactivate generic profile checking for a class using SETROPTS NOGENERIC, RACF deactivates generic profile checking for all classes in the CDT that have the same POSIT value as

the class you specify, except grouping classes. For example, the resource classes TIMS and AIMS and the grouping class GIMS all have a POSIT value of 4 in their respective CDT entries. If you deactivate generic profile checking for TIMS, you will also deactivate it for AIMS. However, GIMS is unaffected because it is a grouping class.

For more information, see the description of the ICHERCDE macro in *z/VM: RACF Security Server Macros and Interfaces*.

GENERICOWNER | NOGENERICOWNER

GENERICOWNER
restricts creation of profiles for general resources.

To create a profile that is more specific than any existing profile protecting the same resource a user must:

- Have the SPECIAL attribute
- Be the owner of the existing profile
- Have the GROUP-special attribute if a group owns the profile
- Have the GROUP-special attribute if the owner of the profile is in the group.

Note:

1. GENERICOWNER provides protection only when there is an existing (less-specific) profile protecting the resource.
2. A less-specific profile must end in * or **. A more-specific profile is a profile that matches the less-specific profile name, character for character, up to the ending * or ** in the less-specific name.

   For example: To allow USERX to RDEFINE A.B in the JESSPOOL class, you need profile A.* in the JESSPOOL class, which is owned by USERX. You also need profile **, owned by the system administrator, to prevent other CLAUTH users from being able to RDEFINE A.B.

   For additional information, see " Permitting Profiles for GENERICOWNER Classes" on page 341.
3. GENERICOWNER does not prevent the creation of a more specific profile if the more specific profile is created in the grouping class and is specified on the ADDMEM operand. For example, profile A* exists in the TERMINAL class and is owned by a group for which user ELAINE does not have group-SPECIAL, If the GENERICOWNER option is in effect, user ELAINE cannot define a more specific profile in the member class (such as, RDEF TERMINAL AA*), but user ELAINE can define a profile if it is specified on the ADDMEM operand for the grouping class profile (such as, RDEF GTERMINL profile-name ADDMEM(AA*)).

NOGENERICOWNER
cancels the restriction on the creation of profiles for general resources.

NOGENERICOWNER is in effect when RACF is using a newly-initialized database.

| NOGENLIST

GENLIST(*class-name* ...)
Also see RACLIST operand.

activates the sharing of in-storage generic profiles for the classes specified. Activate this function for general resource classes defined in the class descriptor table (CDT) that contain a small number of frequently referenced generic profiles. The following classes can be used with GENLIST:

```
APPL       FACILITY    INFOMAN     SDSF        VMCMD    VMRDR
DASDVOL    FIELD       JESJOBS     TERMINAL    VMLAN    VMSEGMT
DSNR       GINFOMAN    RACFEVNT    VMBATCH     VMMDISK  VMNODE
```

When you activate GENLIST processing for a class, a generic profile in that class is copied from the RACF database into common storage the first time an authorized user requests access to a

resource protected by the profile. The profile is retained in common storage and is available for all authorized users, thus saving real storage because the need to retain multiple copies of the same profile (one copy for each requesting user) in common storage is eliminated. Also, because RACF does not have to retrieve the profile each time a user requests access to a resource protected by it, this function saves processing overhead.

If you want to refresh shared in-storage generic profiles for a specific resource class, issue the SETROPTS command with the GENERIC(*class-name*) and REFRESH operands.

Note: RACF does not allow you to specify SETROPTS GENLIST and SETROPTS RACLIST for the same general resource class.

NOGENLIST(*class-name* ...)
Also see NORACLIST operand.

deactivates the sharing of in-storage generic profiles for the classes specified. Deactivate this function for general resource classes defined in the class descriptor table (CDT) that are eligible for GENLIST processing. These classes are listed under the description for GENLIST.

When you specify NOGENLIST, RACF deletes in-storage generic profiles for the specified classes from common storage.

NOGENLIST is in effect for all classes defined in the CDT at RACF initialization.

GLOBAL | NOGLOBAL

GLOBAL(*class-name* ...|*)
specifies those classes eligible for global access checking. Valid class names you can specify are DATASET and all class names defined in the class descriptor table (CDT) except grouping classes. If you specify an asterisk (*), you activate global access checking for the DATASET class plus all the classes in the CDT except grouping classes. For a list of general resource classes defined in the IBM-supplied CDT, see Appendix B, “IBM-Supplied Resource Classes that Apply to z/VM Systems,” on page 349.

If you specify GLOBAL with REFRESH, only those currently active and authorized classes are refreshed. If you have deleted the GLOBAL profile for a CLASS, you should issue the SETROPTS command with the NOGLOBAL keyword specified, rather than GLOBAL with REFRESH specified.

Note:

1. If you activate global access checking for a class using SETROPTS GLOBAL, RACF activates global access checking for all classes in the CDT that have the same POSIT value as the class you specify, except grouping classes. For example, the resource classes TIMS and AIMS and the grouping class GIMS all have a POSIT value of 4 in their respective CDT entries. If you activate global access checking for TIMS, you will also activate it for AIMS. However, you cannot activate this option for GIMS because GIMS is a grouping class.

   For more information, see the description of the ICHERCDE macro in *z/VM: RACF Security Server Macros and Interfaces*.
2. RACF does not automatically propagate the SETROPTS command to non-cluster systems sharing the database for the combination of the GLOBAL and REFRESH options. For this combination of options, the SETROPTS command must be issued to each system sharing the database. See Note “2” on page 289 for more information.

NOGLOBAL(*class-name* ...|*)
deactivates global access checking for the specified classes. Valid class names you can specify are DATASET and all class names defined in the class descriptor table (CDT) except grouping classes. If you specify an asterisk (*), you deactivate global access checking for the DATASET class plus all the classes in the CDT (excluding grouping classes). For a list of general resource classes defined in the IBM-supplied CDT, see Appendix B, “IBM-Supplied Resource Classes that Apply to z/VM Systems,” on page 349.

NOGLOBAL(*) is in effect when RACF is first installed.

Note: If you deactivate global access checking for a class using SETROPTS NOGLOBAL, RACF deactivates global access checking for all classes in the CDT that have the same POSIT value as the class you specify, except grouping classes. For example, the resource classes TIMS and AIMS and the grouping class GIMS all have a POSIT value of 4 in their respective CDT entries. If you deactivate global access checking for TIMS, you will also deactivate it for AIMS. However, GIMS is unaffected because it is a grouping class.

For more information, see the description of the ICHERCDE macro in *z/VM: RACF Security Server Macros and Interfaces*.

GRPLIST | NOGRPLIST

GRPLIST
specifies that RACHECK and FRACHECK processing is to perform list-of-groups access checking for all system users. When you specify GRPLIST, a user's authority to access a resource is not based only on the authority of the user's current connect group; access is based on the authority of any group to which the user is connected.

NOGRPLIST
specifies that the user's authority to access a resource is based on the authority of the user's current connect group. NOGRPLIST is in effect when RACF is first installed.

INACTIVE | NOINACTIVE

INACTIVE(*unused-userid-interval*)
specifies the number of days (1 to 255) that a user ID can remain unused and still be considered valid. RACINIT checks the number of days since the last successful invocation of RACINIT against the INACTIVE value and, if the former is larger, revokes the user's right to use the system. If you specify INACTIVE, INITSTATS must be in effect. If you are using this option, you should copy your primary database to the backup database on a regular basis.

If the backup database is needed but does not contain current information, some user IDs may be revoked because they will appear to have been unused beyond the number of days specified on the INACTIVE operand. For more information, see *z/VM: RACF Security Server System Programmer's Guide*.

NOINACTIVE
specifies that the RACINIT is not to check user IDs against an *unused-userid-interval*.

NOINACTIVE is in effect when RACF is first installed.

INITSTATS | NOINITSTATS

INITSTATS
specifies that statistics available during RACINIT SVC processing are to be recorded. These statistics include the date and time RACINIT is issued for a particular user, the number of RACINITs for a user to a particular group, and the date and time of the last RACINIT for a user to a particular group. If you specify INACTIVE, REVOKE, or WARNING, INITSTATS must be in effect.

INITSTATS is in effect when RACF is first installed.

NOINITSTATS
specifies that statistics available during RACINIT SVC processing are not to be recorded.

JES
Note: *This operand applies to z/OS systems only.*

controls job entry subsystem (JES) options. The JES options are:

BATCHALLRACF | NOBATCHALLRACF

BATCHALLRACF
specifies that JES is to test for the presence of a user ID and password on the job statement or for propagated RACF identification information for all batch jobs. If the test fails, JES is to fail the job.

NOBATCHALLRACF
specifies that JES is not to test for the presence of a user ID and a password on the statement, or propagated RACF identification information for all batch jobs.

NOBATCHALLRACF is in effect when RACF is first installed.

EARLYVERIFY | NOEARLYVERIFY

EARLYVERIFY
specifies that JES is to invoke the system authorization facility (SAF) for jobs that do not qualify for user identification propagation. SAF can call an installation-written exit routine (if installed) for further verification of the user ID, group, and password (if specified) at job submission time. See *z/VM: RACF Security Server System Programmer's Guide* for further information about the z/OS router exit.

NOEARLYVERIFY
specifies that the RACF CVT indicator is not to be set and SAF is not to get control.

NOEARLYVERIFY is in effect when RACF is first installed.

NOEARLYVERIFY has no effect if you are using JES 3.1.3.

XBMALLRACF | NOXBMALLRACF

XBMALLRACF
specifies that JES is to test for the presence of either a user ID and password on the JOB statement, or JES-propagated RACF identification information for all jobs to be run with an execution batch monitor. If the test fails, JES is to fail the job.

XBMALLRACF is only used on JES2.

NOXBMALLRACF
specifies that JES is not to test for the presence of either a user ID and password on the JOB statement, or JES-propagated RACF identification information for all jobs to be run with an execution batch monitor.

NOXBMALLRACF is in effect when RACF is first installed.

NJEUSERID(*userid*)
defines the name (user ID) associated with SYSOUT or jobs that arrive through the network without an RTOKEN or UTOKEN.

The initial user ID (default user ID) after RACF data set initialization is ???????? (eight question marks).

Note: The variable *userid* cannot be a user ID defined in the RACF database. For more information, see the section on providing security for JES in *z/VM: RACF Security Server Security Administrator's Guide*.

UNDEFINEDUSER(*userid*)
defines the name(user ID) that will be associated with local jobs that enter the system without a user ID.

The initial user ID (default user ID) after RACF data set initialization is ++++++++ (eight plus signs).

Note: The variable *userid* cannot be a user ID defined in the RACF database. For more information, see the section on providing security for JES in *z/VM: RACF Security Server Security Administrator's Guide*.

LANGUAGE
Note: *These operands apply to z/OS systems only.*

specifies the system-wide defaults for national languages (such as American English or Japanese) to be used on your system. You can specify a primary language, a secondary language, or both. The languages you specify depend on which products, when installed on your system, check for primary and secondary languages (using RACROUTE REQUEST=EXTRACT):

- If this user will establish an extended MCS console session, the languages you specify should be the same as the languages specified on the LANGUAGE LANGCODE statements in the MMSLSTxx PARMLIB member. See your z/OS system programmer for this information.
- If this is a CICS user, see your CICS administrator for the languages supported by CICS on your system.

The SETROPTS LANGUAGE operand does not affect the language in which the RACF ISPF panels are displayed. The order in which the RACF ISPF panel libraries are allocated determines the language used. If your installation ordered a translated feature of RACF, the RACF program directory gives instructions for setting up the ISPF panels.

PRIMARY(*language*)
specifies the installation's default primary language.

The variable *language* can be a quoted or unquoted string.

If the PRIMARY suboperand is not specified, the primary language is not changed.

SECONDARY(*language*)
specifies the installation's default secondary language.

The language name can be a quoted or unquoted string.

If the SECONDARY suboperand is not specified, the secondary language is not changed.

Note:

1. For both the PRIMARY and SECONDARY suboperands, specify the installation-defined name of a currently active language (a maximum of 24 characters) or one of the language codes (3 characters in length) that is installed on your system. For a list of valid codes, see *National Language Design Guide, National Language Support Reference Manual Volume 2*, SE09-8002.
2. If RACF is not running under MVS/ESA SP Release 4.1 or later, or if the z/OS message service is not active, or if it is running under z/VM, the PRIMARY and SECONDARY values must be a 3-character language code.
3. The same language can be specified for both PRIMARY and SECONDARY.
4. RACF is shipped with both the primary and secondary language defaults set to ENU, meaning United States English.

LIST
specifies that the current RACF options are to be displayed. If you specify operands in addition to LIST on the SETROPTS command, RACF processes the other operands before it displays the current set of options.

You must have the SPECIAL, AUDITOR, group-SPECIAL, or group-AUDITOR attribute to enter the LIST operand.

If you have the SPECIAL or group-SPECIAL attribute, RACF displays all operands except these auditing operands:

- APPLAUDIT | NOAPPLAUDIT
- AUDIT | NOAUDIT
- CMDVIOL | NOCMDVIOL
- LOGOPTIONS
- OPERAUDIT | NOOPERAUDIT
- SAUDIT | NOSAUDIT
- SECLABELAUDIT | NOSECLABELAUDIT.

If you have the AUDITOR, ROAUDIT, or group-AUDITOR attribute, RACF displays all operands.

LOGOPTIONS (*auditing-level* (*class-name...*) ...)
audits access attempts to resources in specified classes according to the auditing-level specified. You must have the AUDITOR attribute. You can specify the DATASET class and any classes in the class

descriptor table (CDT) that have been activated. The resources need not have profiles created in order for auditing to occur.

The SUCCESSES and FAILURES operands result in auditing in addition to any auditing specified in profiles in the class. In contrast, the ALWAYS and NEVER operands override any auditing specified in profiles in the class. Note that LOG=NONE, specified on a RACROUTE REQUEST=AUTH, takes precedence (auditing is not performed).

auditing-level
specifies the access attempts to be logged for *class-name*. These options are processed in the order listed below. Thus, if *class-name* is specified with both SUCCESSES and ALWAYS in the same command, auditing will take place at the SUCCESSES level because option SUCCESSES is processed after ALWAYS.

ALWAYS
All access attempts to resources protected by the class are audited.

NEVER
No access attempts to resources protected by the class are audited. (All auditing is suppressed.)

SUCCESSES
All successful access attempts to resources protected by the class are audited.

FAILURES
All failed access attempts to resources protected by the class are audited.

DEFAULT
Auditing is controlled by the profile protecting the resource, if a profile exists. You can specify DEFAULT for all classes by specifying an asterisk (*) with DEFAULT.

LOGOPTIONS(DEFAULT) is in effect when RACF is first installed.

class-name
the RACF class to which *auditing-level* applies. *Class-name* can be DATASET and any classes in the CDT which have been activated. Each class can have only one auditing level associated with it. The auditing-levels are processed in the following order:

1. ALWAYS
2. NEVER
3. SUCCESSES
4. FAILURES
5. DEFAULT

This processing order occurs independently of the order you specify the auditing-levels. If you specify two or more auditing-levels for a class in the same command, *only the last option processed will take effect.* Thus, if you specify the following command:

```
SETR LOGOPTIONS ( FAILURES ( DATASET, SECLABEL ),
                  ALWAYS ( DATASET, APPL ),
                  DEFAULT (DATASET, GLOBAL )  )
```

The options in effect for the classes will be:

ALWAYS — APPL
FAILURES — SECLABEL
DEFAULT — DATASET, GLOBAL

Classes DATASET and APPL are first assigned auditing-level ALWAYS. Class DATASET is then assigned auditing-level FAILURES, as is class SECLABEL. Finally, class DATASET is assigned DEFAULT auditing-level, as is class GLOBAL.

If you specify one *auditing-level* for *class-name* and in a separate command specify a new auditing level for the same class name, the new auditing level will take effect.

SETROPTS LOGOPTIONS(DEFAULT(*)) is the equivalent to previous versions of RACF. It is in effect when RACF is first installed.

MLACTIVE | NOMLACTIVE
For the relationships among SECLABEL, MLS, MLACTIVE, and MLQUIET, see *z/VM: RACF Security Server Security Administrator's Guide*.

MLACTIVE (FAILURES | WARNING)
causes security labels to be required on all work entering the system and on all resources defined to USER, DATASET, and all classes defined in the class descriptor table that require SECLABEL.

This option is available only if the SECLABEL class is active.

FAILURES
specifies that RACF is to reject any request to create or access any resource which requires a SECLABEL in the profile that protects it, and does not have one, and to reject any work entering the system which does not have a SECLABEL.

The only exception is if MLS(FAILURES) and MLACTIVE(FAILURES) are in effect, and a privileged started task or a user with the SPECIAL attribute and the SYSHIGH SECLABEL attempts to access a resource that requires a SECLABEL and does not have one. In this case, RACF allows the request as long as the request will not declassify data.

MLACTIVE(FAILURES) is the default value.

WARNING
specifies that, when a user requests access to a resource that does not have a SECLABEL and the resource belongs to a class that requires SECLABELs, access is allowed but a warning is issued. Also, when work enters the system without a SECLABEL, access is allowed but a warning is issued.

NOMLACTIVE
allows work to enter the system without a SECLABEL and allows requests to access a resource that does not have a SECLABEL and the resource belongs to a class that requires SECLABELs.

NOMLACTIVE is in effect when RACF is first installed.

MLQUIET | NOMLQUIET
For the relationships among SECLABEL, MLS, MLACTIVE, and MLQUIET, see *z/VM: RACF Security Server Security Administrator's Guide*.

MLQUIET
allows only started procedures, console operators, or users with the RACF SPECIAL attribute to log on, start new jobs, or access resources. Actions requiring use of the RACINIT, RACHECK, or RACDEF macros are available only to the security administrator (RACF SPECIAL user), a trusted computer base job (as indicated in the token), or the console operator.

When this option is enabled, the system is in a tranquil state.

NOMLQUIET
allows all users access to the system.

NOMLQUIET is in effect when RACF is first installed.

MLS | NOMLS
For the relationships among SECLABEL, MLS, MLACTIVE, and MLQUIET, see *z/VM: RACF Security Server Security Administrator's Guide*.

MLS (FAILURES | WARNING)
prevents a user from declassifying data. In order to copy data, the SECLABEL of the target must encompass the SECLABEL of the source.

This option is available only if the SECLABEL class is active.

FAILURES
specifies that RACF is to reject any request to declassify data.

MLS(FAILURES) is the default value if you do not specify either FAILURES or WARNING.

WARNING
specifies that when a user attempts to declassify data, RACF is to allow the request but issue warning messages to the user and the security administrator.

NOMLS
allows users to declassify data within the same CATEGORY.

NOMLS is in effect when RACF is first installed.

MLSTABLE | NOMLSTABLE

MLSTABLE
allows the installation to indicate that no one on the system will be allowed to alter the SECLABEL of an object or alter the definition of the SECLABEL, unless MLQUIET is in effect.

NOMLSTABLE
allows the alteration of SECLABEL definitions or the SECLABELs within a profile without requiring MLQUIET to be in effect.

NOMLSTABLE is in effect when RACF is first installed.

MODEL | NOMODEL
Note: *These operands apply to z/OS systems only.*

MODEL
specifies, through the following suboperands, the model profile processing options. For information about automatic profile modeling, refer to the *z/VM: RACF Security Server Security Administrator's Guide*.

GDG | NOGDG
specifies that each member of a generation data group (GDG) can use a common profile identified by the GDG data set base name. When MODEL(GDG) is in effect and RACHECK processes a GDG data set, it first looks for a base name profile in the RACF database, and, if one exists, uses this common profile. If the GDG base name is not defined in the RACF database, RACHECK uses the profile for the individual GDG name.

NOGDG specifies that RACDEF is not to use a common profile for a new GDG data set.

GROUP | NOGROUP
specifies that RACDEF is to use a model data set profile to complete the profile information for all group-named data sets.

NOGROUP specifies that RACDEF is not to use a model profile for new group-named data sets.

USER | NOUSER
specifies that RACDEF is to use a model data set profile to complete the profile information for all user ID-named data set.

NOUSER specifies that RACDEF is not to use a model data set profile for new user ID-named data sets.

NOMODEL
specifies that there is no model profile processing for GDG, GROUP, or USER data sets.

NOMODEL is in effect when RACF is first installed.

OPERAUDIT | NOOPERAUDIT
specifies whether RACF is to log all actions allowed only because a user has the OPERATIONS (or group-OPERATIONS) attribute. You must have the AUDITOR attribute to enter these operands.

OPERAUDIT
specifies that RACF is to log all actions, such as accesses to resources and commands, allowed only because a user has the OPERATIONS or group-OPERATIONS attribute.

NOOPERAUDIT
specifies that RACF is not to log the actions allowed only because a user has the OPERATIONS or group-OPERATIONS attribute.

NOOPERAUDIT is in effect when RACF is first installed.

PASSWORD (*suboperands*)
specifies a number of suboperands to monitor and check passwords and password phrases:

ALGORITHM(KDFAES) | NOALGORITHM

ALGORITHM(KDFAES)
indicates that RACF should start using the KDFAES algorithm to encrypt user passwords and password phrases. After enablement, the existing algorithm continues to be used to evaluate a user's password or password phrase until the user's password or password phrase is changed. The first time a user's password or password phrase is changed, the new algorithm is used from that point forward.

The KDFAES algorithm is more secure than DES, but is more computationally intensive, by design.

The PWCONVERT keyword of ALTUSER can be used to convert a user's password from DES to KDFAES format without requiring the password to be changed.

If ALGORITHM is specified without a sub-operand, it is ignored.

NOALGORITHM
indicates that the legacy algorithm is used to encrypt passwords. This is the default setting. In this case, the algorithm in effect is determined by the ICHDEX01 exit, with DES being the default if there is no exit installed.

If you deactivate KDFAES after some set of passwords have been encrypted using KDFAES, each password continues to be evaluated using KDFAES. When the password is changed, the legacy algorithm is used from that point forward. Any history entries that were created with KDFAES continue to be evaluated using KDFAES. The PWCONVERT keyword of ALTUSER can be used to delete KDFAES history entries, if you want, after reverting to DES.

HISTORY(*number-previous-values*) | NOHISTORY

HISTORY specifies the number of previous passwords and password phrases (1 to 32) that RACF saves for each user ID and compares with an intended new value. If there is a match with one of these previous values, or with the current value, RACF rejects the intended new password or password phrase.

If you increase the HISTORY number, RACF saves and compares that number of values to the new entry. If you reduce the HISTORY number, values in the user profile that are beyond the newly specified HISTORY number are not deleted and will continue to be used for comparison.

For example, if the HISTORY number is 12 and you reduce that HISTORY number to 8, RACF will also compare the old values 9 through 12 with the intended new password or password phrase. The PWCLEAN keyword of the ALTUSER command can be used to delete those old values.

NOHISTORY specifies that new password or password phrase information is only compared with the current value. If prior history information exists, it is neither deleted nor changed. ALTUSER PWCLEAN can be used to delete history from USER profiles when NOHISTORY is in effect.

NOHISTORY is in effect when RACF is first installed.

INTERVAL(*maximum-change-interval*)
specifies the maximum number of days (1 to 254) that each user's password or password phrase is valid. The value specified for *maximum-change-interval* becomes the following:

- A default value for new users defined to RACF through the ADDUSER command.
- An upper limit for users who specify the INTERVAL keyword on the PASSWORD command.

When a user logs on to the system, RACF compares the system maximum interval value with the maximum interval value specified in the user's profile. RACF uses the lower of the two values to determine if the user's password or password phrase has expired.

The initial default at RACF initialization is 30 days. The maximum change interval cannot be less than the minimum change interval set with the MINCHANGE keyword.

MINCHANGE(*minimum-change-interval*)
specifies the number of days that must pass between a user's password and password phrase changes. Acceptable values are 0 - 254 (days), providing the number of days between changes does not exceed the maximum change interval specified by the INTERVAL keyword. For example, if you specify 5 for your MINCHANGE number, users cannot change their passwords more than once in 5 days, nor can they change their password phrases (if assigned) more than once in 5 days.

The initial default is 0 days, allowing users to change their passwords and password phrases more than once on the same day.

Users can not change their own passwords and password phrases within the minimum change interval. However, you can use the ALTUSER command to change another user's password within the minimum change interval if you have at least one of the following authorities:

- You have the SPECIAL attribute.
- The user is within the scope of a group in which you have the group-SPECIAL attribute.
- You are the owner of the user's profile.
- You have at least CONTROL authority to the IRR.PASSWORD.RESET resource in the FACILITY class, and the other user does not have the SPECIAL, OPERATIONS, AUDITOR, or PROTECTED attribute.
- You have at least CONTROL access to an appropriate resource in the FACILITY class (IRR.PWRESET.OWNER.owner or IRR.PWRESET.TREE.owner), and both of the following conditions are also true:
  - The other user does not have the SPECIAL, OPERATIONS, AUDITOR, or PROTECTED attribute.
  - You are not excluded from altering the user by the IRR.PWRESET.EXCLUDE.excluded-user resource in the FACILITY class.

    For more information about the IRR.PWRESET profiles, see *z/VM: RACF Security Server Security Administrator's Guide*.

MIXEDCASE | NOMIXEDCASE

MIXEDCASE
Indicates that all applications on this system and those that share the RACF database support mixed-case and lowercase passwords. The syntax rules must be modified to allow mixed-case and lowercase characters. (See the RULE section on page "RULEn | NORULEn | NORULES" on page 309 for more information.) When this option is activated, the RACF ALTUSER, ADDUSER, and PASSWORD commands do not translate passwords to uppercase, nor do applications that provide mixed-case password support, such as the z/VM LOGON command, and various TCP/IP applications such as FTP and TELNET. This option is inactive by default.

Important: The MIXEDCASE option is intended to be activated after evaluating and updating applications and implementing appropriate password syntax rules and never deactivated. Deactivate it only if problems are encountered. If you deactivate MIXEDCASE after it was active, any users who changed their passwords to mixed or lower case (when MIXEDCASE was active) will no longer be able to enter the system until an authorized user resets their passwords to uppercase. If you subsequently reactivate MIXEDCASE, the same users must enter their passwords in upper case.

NOMIXEDCASE
Indicates that mixed-case and lowercase passwords are not supported. This is the default setting.

Important: If you issue SETR NOMIXEDCASE after MIXEDCASE was active, any users who changed their passwords to mixed-case or lowercase (when MIXEDCASE was active) can no longer enter the system until an authorized user resets their passwords to uppercase. See the important note for the MIXEDCASE operand.

REVOKE | NOREVOKE

REVOKE(*number-of-unsuccessful-attempts*)
Specifies the number of consecutive unsuccessful attempts (1 - 255) to access the system (using an incorrect password or password phrase) before RACF revokes the user ID on the next unsuccessful attempt. If you specify REVOKE, INITSTATS must be in effect.

The REVOKE number you specify applies to the combination of incorrect passwords and password phrases RACF allows. For example, if you specify 5 as your REVOKE number, a user will be revoked upon three consecutive incorrect passwords followed by three consecutive incorrect password phrases.

Note: The REVOKE count is not incremented if a user that has neither a password nor a password phrase attempts to enter the system with a password or password phrase.

NOREVOKE
Specifies that RACF ignores the number of consecutive unsuccessful attempts to access the system using an incorrect password or password phrase.

RULE*n* | NORULE*n* | NORULES
Note: You might find the ISPF panels easier to use for entering password rules.

RULE*n* (LENGTH (*m1*:*m2*) *content-keyword*(*position*))
specifies an individual syntax rule for new passwords that users specify at logon or on the PASSWORD command. The rule also applies to passwords specified on the ALTUSER commands that have the NOEXPIRED operand. Eight syntax rules are allowed. Therefore, for the RULE*n* suboperand, the value of *n* is 1 - 8.

These syntax rules do not apply to:

- Password phrases
- Logon passwords that are currently in effect for a user
- Logon passwords specified on the ADDUSER command
- Logon passwords specified on the ALTUSER command with the PASSWORD operand and with the EXPIRED operand either specified or defaulted

If multiple rules are defined, a password that passes at least one rule is accepted.

Restriction: Changes to password syntax rules will not force users to immediately change their passwords. RACF does not apply new password rules to users until users change their passwords - either voluntarily or at password expiration.

LENGTH(*m1*:*m2*)
specifies the minimum and maximum password lengths to which this particular rule applies (*m2* must be greater than or equal to *m1*). Because RACF allows passwords no longer than 8 alphanumeric characters, the value for *m2* must be less than or equal to 8. If you omit the *m2* value, the rule applies to a password of one length only.

***content-keyword*(*position*)**
specifies the syntax rules for the positions indicated by the LENGTH suboperand. Rules specifying mixed-case characters should only be set when the MIXEDCASE option is in effect. New passwords will not match these rules when mixed-case passwords are not supported, either because the MIXEDCASE option is not in effect or because an application is used that does not support mixed-case passwords. The possible values for *content-keyword* are:

ALPHA
Includes uppercase alphabetic characters and the national characters # (X'7B'), $ (X'5B'), and @ (X'7C').

ALPHANUM
Includes the ALPHA characters - uppercase alphabetic characters and the national characters # (X'7B'), $ (X'5B'), and @ (X'7C') - and NUMERIC characters.

If the password syntax rule requires only one ALPHANUM character, passwords must contain either one ALPHA character or one NUMERIC character.

If the password syntax rule requires two or more ALPHANUM characters, passwords must contain at least one ALPHA character and at least one NUMERIC character in the specified ALPHANUM positions.

VOWEL
Includes uppercase vowel characters, namely A, E, I, O, and U.

NOVOWEL
Includes characters that are not vowels, such as

- Uppercase alphabetic characters that are consonants, not vowels
- National and special characters
- Numeric characters

CONSONANT
Includes uppercase non-vowel characters.

NUMERIC
Includes numeric characters.

NATIONAL
Includes the national characters # (X'7B'), $ (X'5B'), and @ (X'7C').

MIXEDALL
Includes all the allowable password characters in the following categories. There are either three or four "active" categories, depending on whether SETROPTS PASSWORD(MIXEDCASE) is enabled:

- The national characters, and special characters if SETROPTS PASSWORD(SPECIALCHARS) is in effect.
- Numeric characters
- Uppercase alphabetic characters (not including the national characters)
- Lowercase alphabetic characters, if SETROPTS PASSWORD(MIXEDCASE) is in effect.

MIXEDALL is intended to force a mixture of character types that can include special characters. MIXEDALL requires a character from as many different active categories as there are MIXEDALL positions specified, in any combination:

- When one MIXEDALL position is specified, any character from any active category may be specified in that position. This is equivalent to not specifying a content keyword in this position.
- When two MIXEDALL positions are specified, two characters from any two different active categories must be specified in the designated positions.
- When three MIXEDALL positions are specified, three characters from any three different active categories must be specified in the designated positions.
- When four or more MIXEDALL positions are specified, and SETROPTS PASSWORD(MIXEDCASE) is enabled, then at least one of every category must be specified anywhere across the designated positions. If MIXEDCASE is not enabled, then there is no change in behavior from having three MIXEDALL positions, other than the number of positions over which the three active categories may be spread.

MIXEDCONSONANT
Includes uppercase and lowercase non-vowel characters.

MIXEDVOWEL
Includes the uppercase and lowercase vowel characters, A, E, I, O, U, and a, e, i, o, u.

MIXEDNUM
Includes all characters of the following three types of MIXEDNUM characters:

1. ALPHA characters—includes uppercase alphabetic characters and the national characters # (X'7B'), $ (X'5B'), and @ (X'7C')
2. Lowercase alphabetic characters
3. NUMERIC characters.

If the password syntax rule requires only one MIXEDNUM character, passwords must contain at least one character of *any* one of the three MIXEDNUM character types.

If the password syntax rule requires two MIXEDNUM characters, passwords must contain two characters of *different* MIXEDNUM character types, in one of the following valid combinations:

- An ALPHA character and a lowercase alphabetic
- An ALPHA character and a NUMERIC character
- A lowercase alphabetic character and a NUMERIC character.

If the password syntax rule requires three or more MIXEDNUM characters, passwords must contain three or more MIXEDNUM characters including at least one character of *each* MIXEDNUM character type.

SPECIAL
Includes the special characters documented under SETROPTS PASSWORD(SPECIALCHARS), as well as the national characters # (X'7B'), $ (X'5B'), and @ (X'7C').

If the values in the *content-keywords* do not define every position specified by the LENGTH value, the undefined positions can consist of any combination of alphanumeric characters.

Each *content-keyword* is followed by a position (in the form of *k*, not greater than 8), list of positions (form of *k1,k2,k3...* in any order), or a range (form of *k4:k5*, where *k5* must be greater than or equal to *k4*).

- **Example:**

```
RULE1(LENGTH(8) CONSONANT(1,3,5:8) NUMERIC(2,4))
```

- **Result:**

  Syntax RULE1 applies to passwords eight characters in length with consonants in positions 1, 3, 5, 6, 7, and 8 and numbers in positions 2 and 4. The password B2D2GGDD obeys RULE1, and C3PIBOLO does not.

- **Example:**

```
RULE2(LENGTH(6) NATIONAL(3) MIXEDNUM(4:6))
```

- **Result:**

  Syntax RULE2 applies to passwords 6 characters in length with a national character in position 3 and requires an uppercase alphabetic, a lowercase alphabetic, and a numeric in positions 4, 5, and 6. The password AB@1tD obeys RULE2.

NORULE*n*
specifies that RACF is to delete the particular rule identified by *n*.

NORULES
specifies that RACF is to cancel all password syntax rules established by the installation.

NORULES is in effect when RACF is using a newly initialized database.

SPECIALCHARS | NOSPECIALCHARS

SPECIALCHARS
specifies that all applications on this system and those that share the RACF database support the following additional special characters in passwords. This option is inactive by default.

Hexadecimal value	Symbol (using the EBCDIC 1047 code page)
4B	.
4C	<
4E	+
4F	|
50	&
5A	!
5C	*
60	-
6C	%
6D	_
6E	>
6F	?
7A	:
7E	=

NOSPECIALCHARS
specifies that special characters are not allowed in passwords. This is the default setting. If NOSPECIALCHARS is specified after users have already started using special characters in passwords, those users will still be able to log on with their existing password, but will not be able to include special characters in the new password when they change their password.

WARNING(*days-before-password-expires*) | NOWARNING
specifies the number of days (1 to 255) before a password or password phrase expires when RACF is to issue a warning message to a user. If your installation is performing password verification in the RACINIT macro, RACF issues the warning message when the WARNING value exceeds the INTERVAL value. If you don't want the warning with each logon, specify a value for WARNING that is less than the value you specify for INTERVAL. If you specify WARNING, INITSTATS must be in effect.

NOWARNING specifies that RACF is not to issue the warning message for password and password phrase expiration. NOWARNING is in effect when RACF is first installed.

PREFIX | NOPREFIX
Note: *These operands apply to z/OS systems only.*

PREFIX(*prefix*)
activates RACF protection for data sets that have single-qualifier names, and specifies the 1- to 8-character prefix to be used as the high-level qualifier in the internal form of the names. The variable *prefix* should be a predefined group name, and it must not be the high-level qualifier of any actual data sets in the system.

NOPREFIX
deactivates RACF protection for data sets that have single-level names. NOPREFIX is in effect when RACF is first installed.

PROTECTALL | NOPROTECTALL
Note: *These operands apply to z/OS systems only.*

PROTECTALL (FAILURES | WARNING)
activates protect-all processing. When protect-all processing is active, the system automatically rejects any request to create or access a data set that is not RACF-protected. This processing includes DASD data sets, tape data sets, catalogs, and GDG basenames. Temporary data sets that comply with standard z/OS temporary data set naming conventions are excluded from protect-all processing.

Note that PROTECTALL requires all data sets to be RACF-protected. This includes tape data sets if your installation specifies the TAPEDSN operand on the SETROPTS command.

In order for protect-all to work effectively, you must specify GENERIC to activate generic profile checking. Otherwise, RACF would allow users to create or access only data sets protected by discrete profiles. If your installation uses nonstandard names for temporary data sets, you must also predefine entries in the global access checking table that allow these data sets to be created and accessed.

The WARNING suboperand enables you to specify a warning message to the requestor in place of rejecting the request.

FAILURES
specifies that RACF is to reject any request to create or access a data set that is not RACF-protected.

The default value is FAILURES.

If PROTECTALL(FAILURES) is in effect and a privileged started task or a user with the SPECIAL attribute requests access to an unprotected data set, RACF accepts the access request and issues a protect-all warning message.

WARNING
specifies that, when a user requests creation of, or access to, a data set that is not RACF-protected, RACF is to allow the request but issue warning messages to the user and the security administrator.

NOPROTECTALL
specifies that the system is not to check for RACF protection before it processes a request to create or access a data set. NOPROTECTALL means that users can create and access data sets that are not RACF-protected.

NOPROTECTALL is in effect when RACF is first installed.

RACLIST | NORACLIST

RACLIST(*class-name* ...)
Also see GENLIST operand.

activates the sharing of in-storage profiles, both generic and discrete, for the classes specified. Activate this function for a general resource class defined in the class descriptor table (CDT) that contains a small number of frequently referenced profiles for which you cannot use global access checking.

In-storage profiles for the following classes *must be* shared:

```
APPCSERV     CSFKEYS     OPERCMDS     PTKTDATA     SERVAUTH
APPCTP       DEVICES     PROPCNTL     RACFVARS     VTAMAPPL
CSFSERV      NODES       PSFMPL       SECLABEL
```

In-storage profiles for the following classes can be shared:

```
ACCTNUM      DASDVOL     INFOMAN      MQCMDS     STORCLAS     VMDEV
APPCPORT     DLFCLASS    JESSPOOL     MQCONN     SURROGAT     VMLAN
APPCSI       DSNR        JESJOBS      PERFGRP    TERMINAL     VMNODE
APPL         FACILITY    JESINPUT     RACFEVNT   TSOPROC      VMSEGMT
CBIND        FCICSFCT    LFSCLASS     SDSF       VMBATCH      WRITER
CONSOLE      FIELD       MGMTCLAS     SMESSAGE   VMCMD        XFACLIT
```

When you activate RACLIST processing for a class, RACF copies both discrete and generic profiles for that class into common storage. These profiles are available to all authorized users, thereby eliminating the need for RACF to retrieve a profile each time a user requests access to a resource protected by that profile. Thus, when you activate this function, you reduce processing overhead.

If you specify RACLIST with REFRESH, RACF refreshes shared in-storage generic and discrete profiles for the classes specified.

Note:

1. RACF does not automatically propagate the SETROPTS command to non-cluster systems sharing the database for RACLIST option or the combination of the RACLIST and REFRESH options. For this combination of options, the SETROPTS command must be issued to each system sharing the database. See Note "2" on page 289 for more information.
2. RACF does not allow you to specify SETROPTS RACLIST and SETROPTS GENLIST for the same general resource class.
3. When you first activate SETROPTS RACLIST for a class, and you are sharing databases between systems, you must issue SETROPTS RACLIST for one system and SETROPTS RACLIST REFRESH for the other system.

NORACLIST(*class-name ...*)
(Also see the NOGENLIST operand.)

deactivates the sharing of in-storage profiles, both generic and discrete, for the classes specified. Deactivate this function for general resource classes defined in the class descriptor table (CDT) that are eligible for RACLIST processing. For a list of such classes, see the description of the CDT in *z/VM: RACF Security Server Macros and Interfaces*.

When you specify NORACLIST, RACF deletes in-storage generic and discrete profiles for the specified classes from common storage.

NORACLIST is in effect for all classes defined in the CDT when RACF is first installed.

REALDSN | NOREALDSN
Note: *These operands apply to z/OS systems only.*

REALDSN
specifies that RACF is to record, in any SMF log records and operator messages, the real data set name (not the naming-conventions name) used on the data set commands and in the RACHECK and RACDEF macros.

NOREALDSN
specifies that RACF is to record, in any SMF log records and operator messages, the data set names modified according to RACF naming conventions.

NOREALDSN is in effect when RACF is first installed.

REFRESH
refreshes the in-storage generic profiles when specified with GENERIC, GLOBAL or RACLIST; or the in-storage program control tables when specified with WHEN(PROGRAM).

Note: RACF does not automatically propagate the SETROPTS command to non-cluster systems sharing the database for RACLIST option or the combination of the RACLIST and REFRESH options. For this combination of options, the SETROPTS command must be issued to each system sharing the database. See Note "2" on page 289 for more information.

This same rule applies to multiple RACF service machines on a single z/VM system that share the RACF database. Refer to "RAC (Enter RACF Commands on z/VM)" on page 207.

RETPD(*nnnnn*)

Note: *This operand applies to z/OS systems only.*

specifies the default RACF security retention period for tape data sets, where *nnnnn* is a 1- to 5-digit number in the range of 0 through 65533 or 99999 to indicate a data set that never expires. The security retention period is the number of days that RACF protection is to remain in effect for a tape data set; RACF stores the value in the tape data set profile.

If you specify RETPD, you must also specify TAPEDSN to activate tape data set protection. If you omit TAPEDSN, RACF records the value you specify for security retention period in the list of RACF options. However, without tape data set protection activated, this value is meaningless.

If you specify RETPD and TAPEDSN, the value you specify for security retention period is the default for your installation; RACF places the value in each tape data set profile unless the user specifies one of the following:

- An EXPDT in the JCL other than the current date
- An RETPD other than 0 on the ADDSD command.

If you specify TAPEDSN and do not specify RETPD, RACF uses a value of 0 for the default security retention period.

Note: RACF interprets date fields as:

20*yy* when the year is less than 71
19*yy* when the year is 71 or higher

RVARYPW([SWITCH(*switch-pw*)] [STATUS(*status-pw*)])

specifies the passwords that the operator is to use to respond to requests to approve RVARY command processing, where *switch-pw* is the response to a request to switch RACF databases, and *status-pw* is the response to a request to change RACF status. You can specify different passwords for each response. Note that NO is not a valid password for either SWITCH or STATUS.

When RACF is first initialized, the switch password and the status password are both set to YES.

SAUDIT | NOSAUDIT

specify whether RACF is to log all RACF commands issued by users with the SPECIAL or group-SPECIAL attribute. You must have the AUDITOR attribute to enter these operands.

SAUDIT

specifies that RACF is to log all RACF commands (except LISTDSD, LISTGRP, LISTUSER, RLIST, and SEARCH) issued by users with the SPECIAL or group-SPECIAL attribute. SAUDIT is in effect when RACF is first installed.

NOSAUDIT

specifies that RACF is not to log the commands issued by users with the SPECIAL or group-SPECIAL attribute.

SECLABELAUDIT | NOSECLABELAUDIT

You must have the AUDITOR attribute to specify these options.

SECLABELAUDIT

Specifies that the SECLABEL profile's auditing options are to be used in addition to the auditing options specified for the resource profile. This additional auditing occurs whenever an attempt is made to access a resource protected by a profile that has a security label specified.

The SECLABEL profile requires SETROPTS RACLIST processing. If SECLABEL profile audit options are not specified, SECLABEL auditing is not done.

For more information, refer to *z/VM: RACF Security Server Auditor's Guide*.

NOSECLABELAUDIT

disables auditing by SECLABEL.

NOSECLABELAUDIT is in effect when RACF is first installed.

SECLABELCONTROL | NOSECLABELCONTROL

SECLABELCONTROL
limits the users who can specify the SECLABEL operand on RACF commands. Those allowed to specify the operand are:

- Users with the system-SPECIAL attribute can specify the SECLABEL operand on any RACF command
- Users with the group-SPECIAL attribute can specify the SECLABEL on the ADDUSER and ALTUSER commands when adding a user to a group within their scope of control (provided the group-SPECIAL is permitted to the SECLABEL).

NOSECLABELCONTROL
allows any user to change the SECLABEL field in a profile, as long as the user has at least READ access authority to the associated SECLABEL profile.

NOSECLABELCONTROL is in effect when RACF is first installed.

SECLEVELAUDIT | NOSECLEVELAUDIT
You must have the AUDITOR attribute to specify these operands.

SECLEVELAUDIT (*security-level*)
activates auditing of access attempts to all RACF-protected resources based on the specified installation-defined security level. RACF audits all access attempts for the specified security level and higher.

You can specify only a security level name defined by your installation as a SECLEVEL profile in the SECDATA class. (For information on defining security levels, see the description of the RDEFINE and RALTER commands.)

NOSECLEVELAUDIT
deactivates auditing of access attempts to RACF-protected resources based on a security level.

NOSECLEVELAUDIT is in effect when RACF is first installed.

SESSIONINTERVAL | NOSESSIONINTERVAL

SESSIONINTERVAL(*n*)
sets the maximum value that can be specified by RDEFINE or RALTER for session key intervals. This value, *n*, must be from 1 to 32767 (inclusive).

The SESSIONINTERVAL value after RACF data set initialization is 30. This value will be used for:

1. A default if SESSION is specified without INTERVAL or NOINTERVAL on RDEFINE when defining an APPCLU class profile.
2. An upper limit if INTERVAL is specified on RDEFINE or RALTER for APPCLU class profiles.

NOSESSIONINTERVAL
disables the global limit on the number of days before a session key expires. The internal value is set to zero.

STATISTICS | NOSTATISTICS
use these operands to cause RACF to record or not record statistical information for the specified class name. The valid class names are DATASET and those classes defined in the class descriptor table (CDT). For a list of the general resource classes defined in the IBM-supplied CDT, see Appendix B, “IBM-Supplied Resource Classes that Apply to z/VM Systems,” on page 349.

Note: If you activate or deactivate statistics processing for a class, all other classes in the CDT with the same POSIT number will also be activated or deactivated. If, for instance, you activate statistics processing for the TIMS class, statistics processing will be activated for classes AIMS and GIMS because they share POSIT number 5. (For more information, see the description of the ICHERCDE macro in *z/VM: RACF Security Server Macros and Interfaces*).

STATISTICS(*class-name ... | **)
specifies that RACF is to record statistical information for *class-name*.

If you specify an asterisk (*), you activate the recording of statistical information for the DATASET class and all classes defined in the CDT.

At RACF initialization, STATISTICS is in effect for the DATASET, DASDVOL, TAPEVOL, and TERMINAL classes. Because statistics recording has an impact on system performance, it is recommended that you deactivate this option until your installation evaluates the need to use it versus the potential performance impact. For more information, see *z/VM: RACF Security Server System Programmer's Guide*.

See the Note under the STATISTICS|NOSTATISTICS operand for information on the effect of POSIT numbers on activating classes and information related to the release of RACF of your system.

NOSTATISTICS(*class-name ... | **)
specifies the names of the classes to be deleted from those previously defined to have statistical information recorded.

If you specify an asterisk (*), you deactivate the recording of statistical information for the DATASET class and all classes defined in the CDT.

See the Note under the STATISTICS|NOSTATISTICS operand for information on the effect of POSIT numbers on deactivating classes and information related to the release of RACF of your system.

TAPEDSN | NOTAPEDSN
Note: *These operands apply to z/OS systems only.*

TAPEDSN
activates tape data set protection. When tape data set protection is in effect, RACF can protect individual tape data sets as well as tape volumes.

If you activate tape data set protection, you should also activate the TAPEVOL class. If you do not also activate TAPEVOL, RACF does not check the retention period before it deletes a tape data set, and you must provide your own protection for tape data sets that reside on a volume that contains more than one data set.

Before you activate tape data set protection, see *z/VM: RACF Security Server Security Administrator's Guide* for a complete description of the relationship between TAPEDSN and activating the TAPEVOL class.

NOTAPEDSN
deactivates tape data set protection. When NOTAPEDSN is in effect, RACF cannot protect individual tape data sets, though it can protect tape volumes.

NOTAPEDSN is in effect when RACF is first installed.

TERMINAL(READ | NONE)
is used to set the universal access authority (UACC) associated with undefined terminals. If you specify TERMINAL but do not specify READ or NONE, the system will prompt you for a value.

WHEN | NOWHEN
Note: *These operands apply to z/OS systems only.*

WHEN(PROGRAM)
activates RACF program control, which includes both access control to load modules and program access to data sets.

To set up access control to load modules, you must identify your controlled programs by creating a profile for each in the PROGRAM class. To set up program access to data sets, you must add a conditional access list to the profile of each program-accessed data set. Then, when program control is active, RACF ensures that each controlled load module is executed only by callers with the defined authority. RACF also ensures that each program-accessed data set is opened only by users who are listed in the conditional access list with the proper authority and who are executing the program specified in the conditional access list entry.

For more information about program control, see *z/VM: RACF Security Server Security Administrator's Guide*.

Note: The PROGRAM class does not have to be active.

NOWHEN(PROGRAM)
specifies that RACF program control is not to be active. NOWHEN(PROGRAM) is in effect when RACF is first installed.

Examples

SETROPTS Examples for z/OS and z/VM

Example ID	Element	Description
Example 1	Goal	User FRG34 wants to establish logging options that will cause RACF to log all activity in the USER and GROUP classes, log the activities of users with the SPECIAL and group-SPECIAL attributes, log all accesses allowed only because the user has the OPERATIONS or group-OPERATIONS attribute, log all command violations, and audit all attempts to access RACF-protected resources based on the installation-defined security level “SECRET”.
	Assumptions	User FRG34 has the AUDITOR attribute. SECRET is defined as a SECLEVEL profile in the SECDATA class.
	Command	`SETROPTS AUDIT(USER GROUP) OPERAUDIT SECLEVELAUDIT(SECRET)`
	Defaults	SAUDIT CMDVIOL
Example 2	Goal	User RVU03 wants to establish a set of syntax rules for passwords that obey the following rules: • The minimum password length is 4 characters • Four-character passwords must have at least one numeric and one alphabetic character • Five-character passwords must contain at least one numeric character or be completely alphabetic • Passwords of 6 or more characters consist of any combination of alphabetic and numeric characters.
	Assumptions	User RVU03 has the SPECIAL attribute.
	Command	`SETROPTS PASSWORD(RULE1(LENGTH(4:5) ALPHANUM(1:5)) RULE2(LENGTH(5) ALPHA(1:5)) RULE3(LENGTH(6:8) ALPHANUM(1:8)) RULE4(LENGTH(6:8) NUMERIC(1:8)) RULE5(LENGTH(6:8) ALPHA(1:8)))`
	Defaults	None

SETROPTS Examples for z/VM:

Example ID	Element	Description
Example 3	Goal	User ADM1 wants to display the RACF options currently in effect.
	Assumptions	User ADM1 has the SPECIAL and AUDITOR attributes.
	Command	`SETROPTS LIST`
	Defaults	None
	Output	See Figure 31 on page 320.

SETROPTS Examples for z/OS:

Example ID	Element	Description
Example 4	Goal	User RVU02 wants to establish system-wide options for an installation. The installation requires tape data set protection and tape volume protection, and the maximum password interval is to be 60 days. The default RACF security retention period for tape data sets is to be 360 days.
	Assumptions	User RVU02 has the SPECIAL attribute.
	Command	`SETROPTS PASSWORD(INTERVAL(60))` `CLASSACT(TAPEVOL) TAPEDSN RETPD(360)`
	Defaults	None
Example 5	Goal	User ADM1 wants to enable the generic profile checking facility for the DATASET class.
	Assumptions	User ADM1 has the SPECIAL attribute.
	Command	`SETROPTS GENERIC(DATASET)`
	Defaults	None
Example 6	Goal	User ADM1 wants to activate global access checking for the DATASET class.
	Assumptions	User ADM1 has the SPECIAL attribute.
	Command	`SETROPTS GLOBAL(DATASET)`
	Defaults	None
Example 7	Goal	User ADM1 wants to activate erase-on-scratch processing for all resources with a security level of CONFIDENTIAL or higher and set the SWITCH and STATUS passwords for the RVARY command.
	Assumptions	User ADM1 has the special attribute. The CONFIDENTIAL security level name is known to RACF.
	Command	`SETROPTS ERASE(SECLEVEL(CONFIDENTIAL))` `RVARYPW(SWITCH(LINUS) STATUS(LUCY))`
	Defaults	None

Example ID	Element	Description
Example 8	Goal	The RACF system administrator wants to activate installation defaults for the primary and secondary national languages. The primary language will be Japanese and the secondary language will be Canadian French.
	Assumptions	The system administrator has the SPECIAL attribute. RACF is running under MVS/ESA SP Release 4.1 but the message service is not active. The 3-character language code for Japanese is JPN. The language code for Canadian French is FRC.
	Command	`SETROPTS LANGUAGE( PRIMARY(JPN) SECONDARY(FRC) )`
	Defaults	None

```
SETROPTS LIST[1]
RACF STATUS INFORMATION:
  TEMPLATE VERSION : HRF77A0 00000194.00000022
ATTRIBUTES = INITSTATS NOWHEN(PROGRAM)
STATISTICS = NONE
ACTIVE CLASSES = DATASET USER GROUP VMMDISK VMRDR VMBATCH VMLAN VMSEGMT
GENERIC PROFILE CLASSES =  NONE
GENERIC COMMAND CLASSES =  NONE
GENLIST CLASSES =  NONE
GLOBAL CHECKING CLASSES =  NONE
RACLIST CLASSES =  NONE
AUTOMATIC DATASET PROTECTION IS IN EFFECT
ENHANCED GENERIC NAMING IS NOT IN EFFECT
REAL DATA SET NAMES OPTION IS INACTIVE
JES-BATCHALLRACF OPTION IS INACTIVE
JES-XBMALLRACF OPTION IS INACTIVE
JES-EARLYVERIFY OPTION IS INACTIVE
PROTECT-ALL OPTION IS NOT IN EFFECT
TAPE DATA SET PROTECTION IS INACTIVE
SECURITY RETENTION PERIOD IN EFFECT IS     0 DAYS.
ERASE-ON-SCRATCH IS INACTIVE
SINGLE LEVEL NAMES NOT ALLOWED
LIST OF GROUPS ACCESS CHECKING IS INACTIVE.
INACTIVE USERIDS ARE NOT BEING AUTOMATICALLY REVOKED.
NO DATA SET MODELLING BEING DONE.
```

1

The fourth line of this display, “ATTRIBUTES =”, refers to global RACF attributes in effect for the current IPL of the system. These attributes can only be set with the SETROPTS command. They are different from, and should not be confused with, the RACF user attributes described in Chapter 2, “Basic Information for Using RACF Commands,” on page 7.

Figure 31. Output for Example 3: SETROPTS LIST Part 1 of 2

```
PASSWORD PROCESSING OPTIONS:
 THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS LEGACY
 PASSWORD CHANGE INTERVAL IS  30 DAYS.
 PASSWORD MINIMUM CHANGE INTERVAL IS   0 DAYS.
 MIXED CASE PASSWORD SUPPORT IS NOT IN EFFECT
 SPECIAL CHARACTERS ARE NOT ALLOWED.
 NO PASSWORD HISTORY BEING MAINTAINED.
 USERIDS NOT BEING AUTOMATICALLY REVOKED.
 NO PASSWORD EXPIRATION WARNING MESSAGES WILL BE ISSUED.
 NO INSTALLATION PASSWORD SYNTAX RULES ARE PRESENT.
DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.
DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.
SECLABEL CONTROL IS NOT IN EFFECT
GENERIC OWNER ONLY IS NOT IN EFFECT
COMPATIBILITY MODE IS NOT IN EFFECT
MULTI-LEVEL QUIET IS NOT IN EFFECT
MULTI-LEVEL STABLE IS NOT IN EFFECT
MULTI-LEVEL SECURE IS NOT IN EFFECT
MULTI-LEVEL ACTIVE IS NOT IN EFFECT
CATALOGUED DATA SETS ONLY, IS NOT IN EFFECT
USER-ID FOR JES NJEUSERID IS : ????????
USER-ID FOR JES UNDEFINEDUSER IS : ++++++++
PARTNER LU-VERIFICATION SESSIONKEY INTERVAL MAXIMUM/DEFAULT IS    30 DAYS.
ADDCREATOR IS NOT IN EFFECT
PRIMARY LANGUAGE DEFAULT : ENU
SECONDARY LANGUAGE DEFAULT : ENU
```

Figure 32. Output for Example 3: SETROPTS LIST Part 2 of 2

SMF (Specify SMF Recording on z/VM)

System environment

This command applies to z/VM systems only.

Use the CP command SMSG with SMF. You cannot issue SMF using RAC or from a RACF command session.

Purpose

Use the SMF command to switch to another SMF minidisk or to restart SMF recording. You must use the CP command SMSG to enter this command.

Related Commands

- To activate or deactivate RACF on z/VM temporarily, use the SETRACF command as described in "SETRACF (Deactivate/Reactivate RACF on z/VM)" on page 286.
- To activate or deactivate RACF or to work with the RACF database, use the RVARY command as described in "RVARY (Change Status of RACF Database)" on page 261.

Authorization Required

To use the SMF command, your user ID must be defined in the CSTCONS table. For information on adding users to the CSTCONS table, see *z/VM: RACF Security Server System Programmer's Guide*

Syntax

The complete syntax of the SMF command is:

```
SMSG server-name SMF {RESTART | SWITCH}
```

Parameters

server-name
specifies the name of the service machine that you want to work with. RACFVM is the IBM-supplied default.

RESTART
specifies that you want to restart SMF recording if it has been suspended. Before the restart can be successful, the condition that caused the suspension must be corrected.

SWITCH
specifies that you want to switch SMF recording to the alternate SMF minidisk for a RACF server. For the switch to be successful, the alternate minidisk must not contain an SMF data file.

When entering the command, only one space is allowed between the character string SMF and the operands (RESTART or SWITCH).

Examples

Example 1

Operation: User KES01 wants to restart SMF recording on the RACF service machine, RACFVM, following its suspension.

Known: User KES01 is in the CSTCONS table. The condition that led to the suspension of SMF recording has been corrected.

Command:
```
SMSG RACFVM SMF RESTART
```

Defaults: None

Example 2

Operation: User VMVSP01 wants to switch SMF recording to the alternate SMF minidisk for the service machine, RACFVM.

Known: User VMVSP01 is in the CSTCONS table. The alternate SMF minidisk for the service machine, RACFVM, does not have a file named SMF DATA.

Command:
```
SMSG RACFVM SMF SWITCH
```

Defaults: None

SRDIR (Obtain a List of SFS Directory Profiles)

System environment

SFS directories apply to z/VM systems only.

Purpose

Use the SRDIR command to obtain a list of RACF SFS directory profiles.

You can request one or more of the following:

- Profile names that contain a specific character string
- Profiles for directories that have not been referenced for more than a specific number of days
- Profiles that contain a level equal to the level you specify
- Profiles with the WARNING indicator
- Profiles that contain a security level that matches the security level that you specify
- Profiles that contain an access category that matches the access category that you specify
- Profiles that contain a security label that matches the security label that you specify.

If ISPF is installed, you may want to use the RACF panels and select the option of having your output placed in a REXX exec. This option is not available from the command line.

Note: RACF interprets dates with 2 digit years in the following way, YY represents the 2 digit year.

```
IF 70 < YY <= 99 THEN
   The date is interpreted as 19YY
IF 00 <= YY <= 70 THEN
   The date is interpreted as 20YY
```

Related Commands

- To protect an SFS directory with a discrete or generic profile, use the ADDDIR command as described in “ADDDIR (Add SFS Directory Profile)” on page 16.
- To change an SFS directory profile, use the ALTDIR command as described in “ALTDIR (Alter SFS Directory Profile)” on page 66.
- To delete an SFS directory profile, use the DELDIR command as described in “DELDIR (Delete SFS Directory Profile)” on page 134.
- To list the information in the SFS directory profiles, use the LDIRECT command as described in “LDIRECT (List SFS Directory Profile)” on page 148.
- To permit or deny access to a SFS directory profile, use the PERMDIR command as described in “PERMDIR (Maintain SFS Directory Access Lists)” on page 194.

Authorization Required

You must have a sufficient level of authority for each profile selected as the result of your request. The following checks are made until one of the conditions is met:

- You have the SPECIAL attribute.
- You have the AUDITOR or ROAUDIT attribute.
- The profile is within the scope of a group in which you have either the group-SPECIAL or group-AUDITOR attribute.
- You are the owner of the directory.

- Your user ID matches the userid qualifier of the directory profile name.
- You are on the access list for the directory and you have at least READ authority. (If your level of authority is NONE, the directory is not selected.)
- Your current connect group is on the access list and has at least READ authority. (If the group's level of authority is NONE, the directory is not selected.)
- You have the OPERATIONS attribute or the profile is within the scope of a group in which you have the group-OPERATIONS attribute.
- The universal access authority is at least READ.

In addition to the authorization requirements to use the SRDIR command, one of the following must be true to use the USER(userid) operand:

- You have the system-SPECIAL or system-AUDITOR attribute.
- You are the owner of the specified user profile.
- You enter your own user ID on the USER operand.
- If security levels and security categories are being used on your system, RACF checks your security level and categories against those in the specified user profile.
- You have the group-SPECIAL or group-AUDITOR attribute in a group to which the specified user is connected.

Syntax

The complete syntax of the command is as follows:

```
SRDIR                [ AGE(number-of-days) ]
                     [ {GENERIC | NOGENERIC} ]
                     [ {CATEGORY [(category-name) ]
                       | LEVEL(nn)
                       | SECLABEL(seclabel-name)
                       | SECLEVEL [(seclevel-name) ]
                       | WARNING} ]
                     [ FILTER(filter-string) ]
                     [ {MASK({char-1 | *} [ ,char-2]) | NOMASK} ]
                     [ USER(userid) ]
```

Note: This command is an extension of the SEARCH command as it applies to the DIRECTRY class. Other SEARCH parameters, such as VSAM and VOLUME are also accepted on the command, but are not listed here. If they are specified on this command, they will be ignored.

Parameters

AGE(*number-of-days*)
specifies the aging factor to be used as part of the search criteria. Only directories that have not been referenced within the specified *number-of-days* are selected.

You can specify up to 5 digits.

Note: This operand works only for discrete profiles and requires that STATISTICS is enabled system-wide.

GENERIC | NOGENERIC
specifies whether only generic profiles or no generic profiles (that is, only discrete profiles) are to be selected. If neither operand is specified, both profile types are selected.

RACF ignores these operands unless generic profile command processing is enabled.

CATEGORY | LEVEL | SECLABEL | SECLEVEL | WARNING

CATEGORY[(*category-name*)]
specifies that RACF is to select only profiles with an access category that matches the category name that you specify, where *category-name* is an installation-defined name that is a member of the CATEGORY profile in the SECDATA class. If you specify CATEGORY and omit *category-name*, RACF selects only profiles that contain undefined access category names (names that were once known to RACF but that are no longer valid).

LEVEL(*installation-defined-level*)
specifies that RACF is to select only profiles with an *installation-defined-level* that equals the level you specify. You can specify a value for *level* of 0 through 99.

SECLABEL(*seclabel-name*)
specifies that RACF is to select only profiles with a security label name that matches the *seclabel-name* that you specify.

SECLEVEL[(*seclevel-name*)]
specifies that RACF is to select only profiles with a security level name that matches the *seclevel-name* that you specify, where *seclevel-name* is an installation-defined name that is a member of the SECLEVEL profile in the SECDATA class. If you specify SECLEVEL and omit *seclevel-name*, RACF selects only profiles that contain undefined security level names (names that were once known to RACF but that are no longer valid).

WARNING
specifies that only directories with the WARNING indicator are to be selected.

FILTER(*filter-string*)
Also see MASK operand. The FILTER and MASK | NOMASK operands are mutually exclusive.

specifies the string of alphanumeric characters used to search the RACF database. The *filter-string* defines the range of profile names you wish to select from the RACF database. The *filter-string* length must not exceed 153 characters.

When you issue the SRDIR command with the FILTER operand, RACF lists profile names from the RACF database matching the search criteria specified in the filter string. Note that RACF lists only those profile names that you are authorized to see.

The following generic characters have special meaning when used as part of the filter string:

%
You can use the percent sign to represent any **one** character in the profile name, including a generic character.

*****
You can use a single asterisk to represent **zero or more characters in a qualifier**, including generic characters. If you specify a single asterisk as the only character in a qualifier, it represents the entire qualifier.

******
You can use a double asterisk to represent **zero or more qualifiers** in the profile name. You cannot specify other characters with ** within a qualifier. (For example, you can specify FILTER(FP:USER1.**), but not FILTER(FP:USER1.A**). You can also specify ** as the only characters in the filter-string to represent any entire directory profile name.

Note:

1. You can use FILTER as an alternative to MASK | NOMASK as a method for searching the RACF database. FILTER offers more flexibility than MASK. For example, when you use FILTER, you can generalize the character string you specify to match multiple qualifiers or multiple characters within a profile name. You can also specify a character string to match a single character regardless of its value or search for a character string anywhere in a profile name.
2. The filter string must be in SFS profile name format. For example, you can specify FILTER(FP:USER.**) but not FILTER(FP.USER1.**)

3. You cannot use a generic character (*, **, or %) in the FILEPOOLID or USERID qualifier in a directory name when you define a generic profile for a directory. However, you can use a generic character in FILEPOOLID or USERID of a directory name when specifying a filter-string with the FILTER operand.

MASK | NOMASK

The MASK | NOMASK and FILTER operands are mutually exclusive.

MASK(*char-1* | * [,*char-2*])

Also see FILTER operand.

specifies the strings of alphanumeric characters used to search the RACF database. This data defines the range of profile names selected. The two character strings together must not exceed 153 characters.

Note: A colon (:) is not allowed in the MASK operand. Use the FILTER operand to specify names in SFS format.

char-1

Each profile name selected with this command starts with char-1. The string may be any length up to 153 characters. All profile names beginning with char-1 are searched.

If an asterisk (*) is specified for char-1, char-1 will be ignored and char-2 will identify the character string appearing anywhere in the resource name.

char-2

If you specify char-2, the selected profile names include only those names containing char-2 somewhere after the occurrence of char-1. This limits the list to some subset of directory names identified with char-1.

If you omit both the MASK and NOMASK operands, the entire DIRECTRY class is searched. (Note that omitting both operands is the same as NOMASK.)

NOMASK

specifies that RACF is to select all profiles (to which you are authorized) in the DIRECTRY class.

USER(*userid*)

specifies that RACF is to list the SFS directory profiles that the specified user has access to (READ authority or higher, or owner). RACF lists only those profiles that the specified *userid*is allowed to see. For example, if you issue:

```
SRDIR  USER(JONES)
```

RACF lists profiles in the DIRECTRY class that user ID JONES has access to.

Note:

1. You should not specify a user ID that has been revoked. If you need to display information about a user whose user ID is revoked, perform the following steps:
   a. Change the password for the user ID
   b. Resume the user ID
   c. Issue the SRDIR command to display the desired information
   d. Revoke the user ID.
2. You can only specify one user ID at a time on the USER operand.

Examples

Example 1

Operation: To determine what SFS directory profiles user ID JONES has access to.

Known: User JONES is RACF-defined.

Command:
```
SRDIR USER(JONES)
```

Defaults: None

Example 2

Operation: To determine what directory profiles belong to the user ID ADAMS, who has a file pool ID of FP1.

Known: User ADAMS is RACF-defined.

Command:
```
SRDIR FILTER(FP1.ADAMS.**)
```

Defaults: None

SRFILE (Obtain a List of SFS File Profiles)

System environment

SFS files apply to z/VM systems only.

Purpose

Use the SRFILE command to obtain a list of RACF SFS file profiles.

You can request one or more of the following:

- Profile names that contain a specific character string
- Profiles for files that have not been referenced for more than a specific number of days
- Profiles that contain a level equal to the level you specify
- Profiles with the WARNING indicator
- Profiles that contain a security level that matches the security level that you specify
- Profiles that contain an access category that matches the access category that you specify
- Profiles that contain a security label that matches the security label that you specify.

If ISPF is installed, you may want to use the RACF panels and select the option of having your output placed in a REXX exec. This option is not available from the command line.

Note: RACF interprets dates with 2 digit years in the following way, YY represents the 2 digit year.

```
IF 70 < YY <= 99 THEN
   The date is interpreted as 19YY
IF 00 <= YY <= 70 THEN
   The date is interpreted as 20YY
```

Related Commands

- To protect an SFS file with a discrete or generic profile, use the ADDFILE command as described in “ADDFILE (Add SFS File Profile)” on page 22.
- To change an SFS file profile, use the ALTFILE command as described in “ALTFILE (Alter SFS File Profile)” on page 81.
- To delete an SFS file profile, use the DELFILE command as described in “DELFILE (Delete SFS File Profile)” on page 139.
- To list the information in the SFS file profile(s), use the LFILE command as described in “LFILE (List SFS File Profile)” on page 154.
- To permit or deny access to an SFS file, use the PERMFILE command as described in “PERMFILE (Maintain SFS File Access Lists)” on page 198.

Authorization Required

You must have a sufficient level of authority for each profile selected as the result of your request. The following checks are made until one of the conditions is met:

- You have the SPECIAL attribute.
- You have the AUDITOR or ROAUDIT attribute.
- The profile is within the scope of a group in which you have either the group-SPECIAL or group-AUDITOR attribute.
- You are the owner of the file.

- Your user ID matches the userid qualifier of the file profile name.
- You are on the access list for the file and you have at least READ authority. (If your level of authority is NONE, the file is not selected.)
- Your current connect group is on the access list and has at least READ authority. (If the group's level of authority is NONE, the file is not selected.)
- You have the OPERATIONS attribute or the profile is within the scope of a group in which you have the group-OPERATIONS attribute.
- The universal access authority is at least READ.

In addition to the authorization requirements to use the SRFILE command, one of the following must be true to use the USER(userid) operand:

- You have the system-SPECIAL or system-AUDITOR attribute.
- You are the owner of the specified user profile.
- You enter your own user ID on the USER operand.
- If security levels and security categories are being used on your system, RACF checks your security level and categories against those in the specified user profile.
- You have the group-SPECIAL or group-AUDITOR attribute in a group to which the specified user is connected.

Syntax

The complete syntax of the command is:

```
SRFILE                  [ AGE(number-of-days) ]
                        [ {GENERIC | NOGENERIC} ]
                        [ {CATEGORY [(category-name)]
                          | LEVEL(nn)
                          | SECLABEL(seclabel-name)
                          | SECLEVEL [(seclevel-name)]
                          | WARNING} ]
                        [ FILTER(filter-string) ]
                        [ {MASK({char-1 | *} [ ,char-2]) | NOMASK } ]
                        [ USER(userid) ]
```

Note: This command is an extension of the SEARCH command as it applies to the FILE class. Other SEARCH parameters, such as VSAM and VOLUME are also accepted on the command, but are not listed here. If they are specified on this command, they will be ignored.

Parameters

AGE(*number-of-days*)
specifies the aging factor to be used as part of the search criteria. Only files that have not been referenced within the specified number of days are selected.

You can specify up to 5 digits for *number-of-days*.

Note: This operand works only for discrete profiles and requires that STATISTICS is enabled system-wide.

GENERIC | NOGENERIC
specifies whether only generic profiles or no generic profiles (that is, only discrete profiles) are to be selected. If neither operand is specified, both profile types are selected.

RACF ignores these operands unless generic profile command processing is enabled.

CATEGORY | LEVEL | SECLABEL | SECLEVEL | WARNING

CATEGORY[(*category-name*)]
specifies that RACF is to select only profiles with an access category that matches the category name that you specify, where *category-name* is an installation-defined name that is a member of the CATEGORY profile in the SECDATA class. If you specify CATEGORY and omit *category-name*, RACF selects only profiles that contain undefined access category names (names that were once known to RACF but that are no longer valid).

LEVEL(*installation-defined level*)
specifies that RACF is to select only profiles with an *installation-defined-level* that equals the level you specify. You can specify a value for *level* of 0 through 99.

SECLABEL(*seclabel-name*)
specifies that RACF is to select only profiles with a security label name that matches the *seclabel-name* that you specify.

SECLEVEL[(*seclevel-name*)]
specifies that RACF is to select only profiles with a security level name that matches the *seclevel-name* that you specify, where *seclevel-name* is an installation-defined name that is a member of the SECLEVEL profile in the SECDATA class. If you specify SECLEVEL and omit *seclevel-name*, RACF selects only profiles that contain undefined security level names (names that were once known to RACF but that are no longer valid).

WARNING
specifies that only files with the WARNING indicator are to be selected.

FILTER(*filter-string*)
Also see MASK operand. The FILTER and MASK | NOMASK operands are mutually exclusive.

specifies the string of alphanumeric characters used to search the RACF database. The filter string defines the range of profile names you wish to select from the RACF database. The filter string length must not exceed 171 characters.

When you issue the SRFILE command with the FILTER operand, RACF lists profile names from the RACF database matching the search criteria specified in the filter string. Note that RACF lists only those profile names that you are authorized to see.

The following generic characters have special meaning when used as part of the *filter-string*:

%
You can use the percent sign to represent any **one** character in the profile name, including a generic character.

*****
You can use a single asterisk to represent **zero or more characters in a qualifier**, including generic characters. If you specify a single asterisk as the only character in a qualifier, it represents the entire qualifier.

******
You can use a double asterisk to represent **zero or more qualifiers** in the profile name. You cannot specify other characters with ** within a qualifier. (For example, you can specify `FILTER(ONE SCRIPT FP:USER1.**)`, but not `FILTER(ONE SCRIPT FP:USER1.A**)`. You can also specify `* * **` as the only characters in the filter-string to represent any entire file profile name.

Note:

1. You can use FILTER as an alternative to MASK | NOMASK as a method for searching the RACF database. FILTER offers more flexibility than MASK. For example, when you use FILTER, you can generalize the character string you specify to match multiple qualifiers or multiple characters within a profile name. You can also specify a character string to match a single character regardless of its value or search for a character string anywhere in a profile name.
2. The filter string must be in SFS profile name format. For example, you can specify `FILTER(* SCRIPT FP:USER.**)` but not `FILTER(FP.USER1.**.*.SCRIPT)`

3. You cannot use a generic character (*, **, or %) in the FILEPOOLID or USERID qualifier in a file name when you define a generic profile for a file. However, you can use a generic character in FILEPOOLID or USERID of a file name when specifying a filter-string with the FILTER operand.

MASK | NOMASK

The MASK | NOMASK and FILTER operands are mutually exclusive.

MASK(*char-1* | * [,*char-2*])

Also see FILTER operand.

specifies the strings of alphanumeric characters used to search the RACF database. This data defines the range of profile names selected. The two character strings together must not exceed 171 characters.

Note: A colon (:) is not allowed in the MASK operand. Because the MASK operand assumes that the input is in the RACF format, use the FILTER operand to specify names in SFS format.

char-1

Each profile name selected with this command starts with *char-1* in the FILEPOOLID position of the name. The string may be any length up to 171 characters. All profile names beginning with *char-1* in the FILEPOOLID name are searched.

If an asterisk (*) is specified for *char-1*, char-1 will be ignored and char-2 will identify the character string appearing anywhere in the resource name.

char-2

If you specify *char-2*, the selected profile names include only those names containing char-2 somewhere after the occurrence of *char-1*. This limits the list to some subset of file names identified with *char-1*.

If you omit both the MASK and NOMASK operands, the entire FILE class is searched. (Note that omitting both operands is the same as NOMASK.)

NOMASK

specifies that RACF is to select all profiles (to which you are authorized) in the FILE class.

USER(*userid*)

specifies that RACF is to list the SFS file profiles that the specified user has access to (READ authority or higher, or owner). RACF lists only those profiles that the specified *userid*is allowed to see. For example, if you issue:

```
SRFILE  USER(JONES)
```

RACF lists profiles in the FILE class that user ID JONES has access to.

Note:

1. You should not specify a user ID that has been revoked. If you need to display information about a user whose user ID is revoked, perform the following steps:
   a. Change the password for the user ID
   b. Resume the user ID
   c. Issue the SRFILE command to display the desired information
   d. Revoke the user ID.
2. You can only specify one user ID at a time on the USER operand.

Examples

Example 1

Operation: To list all your file profiles.

Known: Your user ID is ADAMS and your file pool ID is FP2.

Command:
```
SRFILE FILTER(* * FP2:ADAMS.**)
```

Defaults: None

Example 2

Operation: User SYSADM wants to list all SFS file profiles in the RESEARCH file pool.

Known: SYSADM has the SPECIAL attribute.

Command:
```
SRFILE FILTER(* * RESEARCH:*.**)
```

Defaults: None

Appendix A. Resource Profile Naming Considerations

Profile Definitions

In RACF, resource profiles contain a description of a resource, including the authorized users and the access authority of each user. Resource profiles can be discrete, generic, or, additionally for the DATASET class, fully-qualified generic.

Discrete Profiles

A *discrete* profile can protect a single resource that has unique security requirements. A discrete profile matches the name of the resource it protects and cannot exist independently of the resource. In the DATASET class, if you delete the resource, you delete the profile.

For example, on z/OS, a profile called `SMITH.REXX.EXEC` in class DATASET would protect the data set named `SMITH.REXX.EXEC`. On z/VM, a profile called `SMITH.191` in class VMMDISK would protect SMITH's 191 disk.

Generic Profiles

A *generic* profile can protect several resources that have a similar naming structure and security requirements. Specify generic characters in the profile name if you want to protect more than one resource with the same security requirements.

One or more of the following generic characters are allowed:

- Percent sign (%)
- Single asterisk (*)
- Double asterisk (**)
- Ampersand (&)

Note:

1. The double asterisk (**) is not allowed with the DATASET class if enhanced generic naming (EGN) is inactive.
2. The ampersand (&) is only for general resource profile names and only if the RACFVARS class is active. Resource profiles can be created to protect resource names with *unlike* names. See *z/VM: RACF Security Server Security Administrator's Guide* for more information.

For example, on z/OS, a profile called `SMITH.*` in class DATASET would protect all of SMITH's data sets that did not have a more specific profile defined (NOEGN is in effect). On z/VM, a profile called `SMITH.*` in class VMMDISK would protect all of SMITH's minidisks that did not have a more specific profile defined.

Fully-Qualified Generic Profiles (DATASET class only)

A *fully-qualified* generic profile matches exactly the name of the data set it protects.

One reason to choose a fully-qualified generic profile for data set protection is that the profile is not deleted if the data set is deleted. If the data set is deleted and then re-created, the protection is there without creating another profile. Another reason is to protect multiple copies with one profile.

Determining RACF Protection

Although multiple generic profiles can match a general resource name, only the most specific profile actually protects it. For example, AB.CD*, AB.CD.**, and AB.**.CD all match the data set AB.CD, but AB.CD* protects the data set.

The best way to determine which profile is protecting a given resource is to use one of the list commands.

To find out what profile is protecting a general resource, enter the RLIST command:

```
RLIST class-name resource-name
```

which looks for a discrete profile. If none is found, and generic profile checking is in effect for the class, the generic profile which protects the resource is displayed.

To find out what profile is protecting your data set, enter:

```
LISTDSD DA('data-set-name')
```

which looks for a discrete profile. If none is found, and generic profile checking is in effect for the DATASET class, enter:

```
LISTDSD DA('data-set-name') GENERIC
```

which looks for a generic profile.

To find out what profile is protecting your SFS file or directory, issue the LFILE command for files and the LDIRECT command for directories.

For information, see *z/VM: RACF Security Server General User's Guide*.

The rest of the appendix discusses the rules governing:

- Profile names for data sets
- Profile names for general resources.
- Profile names for SFS files and directories

Profile Names for Data Sets

Table 2 on page 336 shows the availability of generic characters. The use of the generic character % is not changed by the EGN setting.

Note: Depending on whether or not EGN is active, the ending * has different meanings. These are explained in more detail later in this section.

Table 2. Generic Naming for Data Sets

EGN status	Ending .** Allowed	Middle .**. Allowed	Beginning * Allowed	Middle * Allowed	Ending * Allowed
EGN on	Yes	Yes	No	Yes	Yes
EGN off	No	No	No	Yes	Yes

For naming profiles in the DATASET class on z/OS, you can use discrete, generic, or fully-qualified generic names.

Discrete Profiles

These are the same as TSO data set names (see *TSO/E Command Language Reference*), except that the high-level qualifier (or the qualifier supplied by a command installation exit) must be a valid RACF-defined user ID or group name.

Generic Profile Rules—Enhanced Generic Naming 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 may it contain, a generic character—for example, `*.ABC`, `AB%.B`, and `AB*.AB` are not allowed.

Tables are provided to show the variety of profiles that can be created using generics, using enhanced generic naming, and what happens to the profile protection if enhanced generic naming is turned off.

Table 3 on page 337 and Table 4 on page 337 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 5 on page 338 and Table 6 on page 338 provide examples of data set names with enhanced generic naming (`SETR EGN` is on).

Table 7 on page 339 and Table 8 on page 339 provide examples of data set names if enhanced generic naming is turned off after being turned on. It is not recommended that you turn EGN off after you have turned it on.

Table 3. Generic Naming for Data Sets with Enhanced Generic Naming Inactive—Asterisk 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 4. Generic Naming for Data Sets with Enhanced Generic Naming Inactive—Asterisk in the Middle or %

Profile Name	**ABC.%EF**	**AB.*.CD**	**AB.CD*.EF**
Resources protected by the profile	ABC.DEF ABC.XEF	AB.CD.CD	AB.CDEF.EF AB.CDE.EF
Resources not protected by the profile	ABC.DEFGHI ABC.DEF.GHI ABC.DDEF	AB.CD AB.CD.EF AB.CDEF ABC.DEF ABC.XY.CD AB.XY.XY.CD	AB.CD.XY.EF

Generic Profile Rules—Enhanced Generic Naming Active

The *enhanced generic naming* option applies only to data sets and allows you to use double asterisk (**) 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 will make 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.

  The meaning of an ending asterisk depends on whether the 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.

  RACF does not allow you to specify any generic characters in the high-level qualifier of a data set name.

Table 5 on page 338 and Table 6 on page 338 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 5. Generic Data Set Profile Names Created with Enhanced Generic Naming Active—Asterisk and Double Asterisk at the End

Profile Name	**AB.CD***	**AB.CD.***	**AB.CD.****	**AB.CD*.****	**AB.CD.*.****
Resources protected by the profile	AB.CD AB.CDEF	AB.CD.EF AB.CD.XY	AB.CD AB.CD.EF AB.CD.EF.GH AB.CD.XY	AB.CD AB.CD.EF AB.CDEF AB.CDEF.GH AB.CD.EF.GH AB.CD.XY	AB.CD.EF AB.CD.EF.GH AB.CD.XY
Resources not protected by the profile	AB.CD.EF AB.CD.EF.GH AB.CD.XY ABC.DEF	AB.CD AB.CDEF AB.CD.EF.GH ABC.DEF	AB.CDEF AB.CDE.FG ABC.DEF	ABC.DEF	ABC.DEF AB.CDEF AB.CDEF.GH AB.CD ABC.XY.XY.EF

Table 6. Generic Data Set Profile Names Created with Enhanced Generic Naming Active—Asterisk, Double Asterisk, or Percent Sign 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

Table 6. Generic Data Set Profile Names Created with Enhanced Generic Naming Active—Asterisk, Double Asterisk, or Percent Sign in the Middle (continued)			
Profile Name	**ABC.%EF**	**AB.*.CD**	**AB.**.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 may 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.

Data set profiles created before enhanced generic naming is activated continue to provide the same RACF protection after this option is activated.

If you protect resources with generic profiles while enhanced generic naming is active and then deactivate this option, your resources may no longer be protected. Table 7 on page 339 and Table 8 on page 339 show examples of generic profiles created with enhanced generic naming active and the protection after deactivation.

Table 7. After Deactivating EGN—Asterisk and Percent Sign in the Middle		
Profile Name	**ABC.%EF**	**ABC.*.DEF**
How RACF displays the name after EGN is deactivated	ABC.%EF	ABC.*.DEF
Resources protected by the profile after EGN is deactivated	Same as before	Same as before

Table 8. After Deactivating EGN—Asterisk and Double Asterisk at the End					
Profile Name	**AB.CD***	**AB.CD.***	**AB.CD.****	**AB.CD*.****	**AB.CD.*.****
How RACF displays the name after EGN is deactivated	AB.CD*	AB.CD.*	AB.CD.	AB.CD*	AB.CD.*
Resources protected by the profile after EGN is deactivated	None (!!)	None (!!)	None (as expected)	Same as before	Same as before

Profile Names for General Resources

Table 9 on page 340 shows the availability of generic characters before and with RACF Release 1.9 or later. The usage of the generic character % has not changed.

Note: The ending asterisk has different meanings and is explained further in the appropriate sections.

Table 9. Generic Naming for General Resources				
	Double Asterisk Allowed in Beginning, Middle, or End	**Middle Asterisk Allowed**	**Beginning Asterisk Allowed**	**Ending Asterisk Allowed**
Starting With RACF 1.9	Yes	Yes	Yes	Yes
Prior to RACF 1.9	No	No	No	Yes

For naming general resources, you can use discrete or generic profiles. As mentioned before, discrete profile names exactly match the general resource name.

Valid generic characters are a percent sign (%), asterisk (*), double asterisk (**), and ampersand (&).

- Specify a percent sign to match any single character in a resource profile name
- Specify a double asterisk once in a profile name as follows:
  - As the entire profile name to match all resource names in a class
  - As either a beginning, middle, or ending qualifier (for example, **.ABC, ABC.**.DEF, or ABC.**) to match zero or more qualifiers in a resource name.

    Note: ** is always available for general resources. The SETROPTS EGN setting is exclusively for data sets.
- Specify an asterisk as follows:
  - As a qualifier at the beginning of a profile name to match any one qualifier in a resource name
  - As a character at the end of a profile name (for example, ABC.DEF*) to match zero or more characters until the end of the resource name, zero or more qualifiers until the end of the resource 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 resource name
  - As a qualifier in the middle of a profile name (for example, ABC.*.DEF) to match any one qualifier in a resource 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 resource name.
- Specify an ampersand as follows:
  - In a profile name to indicate that RACF is to use a profile in the RACFVARS class to determine the actual values to use for that part of the profile name.

See *z/VM: RACF Security Server Security Administrator's Guide* for the unique naming conventions of specific classes and for a discussion of the RACFVARS class. See also the product documentation (such as PSF or CICS) for the naming conventions of specific classes.

Restricted Use of %* in General Resources

With RACF Release 1.9 or later, the %* combination requires special attention.

New profiles with an ending %* are no longer allowed, nor are profiles named %*. The RDEFINE command will return an error message.

Existing profiles with an ending %* are usable, but they should be deleted before creating any new profiles with a middle or beginning * or **. The RALTER and RDELETE commands will accept %* to enable you to make the changes.

Instead of using an ending %*, create new profiles ending with %.** or * for similar function (change `AB.C%*` to `AB.C%.**` or `AB.C*`).

If you have existing profiles named %*, you should create new profiles (suggested name **).

Note: When creating the new profiles, consider using the FROM operand for continued use of the same access list.

Table 10 on page 341, Table 11 on page 341, and Table 12 on page 341 give examples of generic profile names for general resources.

Table 10. Generic Naming for General Resources—Percent Sign, Asterisk, or Double Asterisk at the Beginning

Profile Name	**%.AB**	***.AB**	****.AB**
Resources protected by the profile	B.AB A.AB	AB.AB ABC.AB A.AB	AB A.A.A.AB AB.AB A.AB
Resources not protected by the profile	AB.AB ABC.AB	AB.CD AB.C.AB AB	ABC.AB.DEF ABAB

Table 11. Generic Naming for General Resources—Asterisk or Double Asterisk at the Ending

Profile Name	**AB.CD***	**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.XY	AB.CD.CD AB.CD.X.Y.Z AB.CD 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	ABC.CD AB.CDE.EF

Table 12. Generic Naming for General Resources—Asterisk, Double Asterisk, or Percent Sign in the Middle

Profile Name	**ABC.%EF**	**AB.*.CD**	**AB.CD*.CD**	**AB.**.CD**
Resources protected by the profile	ABC.DEF ABC.XEF	AB.CD.CD	AB.CD.CD AB.CDEF.CD	AB.CD AB.X.CD AB.X.Y.CD
Resources not protected by the profile	ABC.DEFGHI ABC.DEF.GHI	AB.CD AB.CD.EF AB.CDEF AB.X.Y.CD	AB.CD.XY AB.CD.XY.CD	AB.CD.EF AB.CDEF ABC.X.CD.EF ABC.DEF ABC.XY.CD ABC.XY.XY.CD

Although multiple generic profiles may match a general resource name, only the most specific actually protects the resource. For example, AB.CD*, AB.CD.**, and AB.**.CD all match the general resource AB.CD, but AB.CD* protects it.

In general, given two profiles that match a general resource, you can find the more specific one by comparing the profile name from left to right. Where they differ, a nongeneric character is more specific than a generic character. In comparing generics, a percent sign is more specific than an asterisk, and an asterisk is more specific than double asterisk. Another way to determine the most specific is with the SEARCH command, as there are some rare exceptions to the general rule. SEARCH will always list the profiles in the order of the most specific to the least specific.

Permitting Profiles for GENERICOWNER Classes

GENERICOWNER gives an installation the ability of restricting CLAUTH users from creating profiles in a class. In order to do this, a top-level ** profile is defined. This profile is owned by the system administrator and this profile blocks all non-SPECIAL users from creating profiles. A *permitting profile* must be defined for each CLAUTH user. Each profile defines the subset of resources in the class that the user is allowed to create.

When a CLAUTH user attempts to define a resource, a search is made for a less-specific (permitting) profile. This less-specific profile is a profile that matches the more-specific profile name, character for character, up to the ending * or ** in the less-specific name.

This definition may appear simple, but is not exactly what you might expect in comparison to the preceding section.

Table 13. Permitting profiles

Profile Name	**AA.***	**AA.****	**AA***	**A.*.B.****
covered	AA.BB AA.B.C	AA.* AA AA.BB AA.B.C	AA.* AA AA.BB AA.B.C AAC.BB	A.*.B.CC
not covered	AA.** AA ABC.BB	AAC.BB ABC.BB	ABC.BB	A.A.B.CC

Profile Names for SFS Files and Directories

Starting with RACF 1.10, you can protect files and directories in the shared filed system (SFS). The RACF classes, FILE and DIRECTRY, must be active to use this support.

Twelve RACF SFS commands are available to manipulate RACF profiles for protecting SFS files and directories. The RACF SFS commands are: ADDDIR, ADDFILE, ALTDIR, ALTFILE, DELDIR, DELFILE, LDIRECT, LFILE, PERMDIR, PERMFILE, SRDIR, and SRFILE.

To enter the file and directory profile names in the RACF SFS commands, the following formats must be used:

```
directory-id  = [file-pool-id:] [userid].[dir1.dir2...dir8]
file-id       =  filename filetype directory-id
```

The operands in brackets are optional. If you enter command in the RACF command session on z/VM, you must specify file pool ID. The maximum length of a valid DIRECTRY profile name is 153 and the maximum length for a valid file name is 171. Qualifiers for the profile names are explained in Table 14 on page 342.

Table 14. Rules for forming the qualifiers of FILE and DIRECTRY names

Qualifier	**Length**	**Characters Allowed**
file pool ID	1-8 characters	A-Z for first character, A-Z and 0-9 for remaining
userid	1-8 characters	A-Z, 0-9, $, #, @
sub-directory (there may be 0 to 8 sub-directory names)	1-16 characters	A-Z, 0-9, $, #, @, and _ (underscore)
file name	1-8 characters	A-Z, 0-9, $, #, @, +, - (hyphen), : (colon), and _ (underscore)
file type	1-8 characters	A-Z, 0-9, $, #, @, +, - (hyphen) : (colon), and _ (underscore)

Note: File names and file types on z/VM may contain lowercase letters; RACF profile names *cannot* contain lowercase letters. To protect SFS files that contain lowercase letters, you must use generic profile names.

For example, to protect the file

```
OFSMAIL OFSLOGfl POOL1:USER1.DIR1 (note the lowercase fl)
```

you could use any of the following file profile names:

```
OFSMAIL OFSLOG*  POOL1:USER1.DIR1
OFSMAIL OFSLOG%% POOL1:USER1.DIR1
```

```
*       OFSLOG%% POOL1:USER1.DIR1
*       OFSLOG%% POOL1:USER1.DIR1.**
```

Default Naming Conventions

Profile names for files and directories contain file pool ID and user ID. In RACF SFS commands issued on z/VM using RAC, either qualifier may be omitted by following SFS standards for naming files and directories. For RACF SFS commands issued on z/VM using the RACF command session, only the user ID may be omitted.

RACF uses the following guidelines when the file pool ID or user ID is omitted from an SFS format profile name in a RACF command:

1. If a RACF SFS command is entered on z/VM using RAC, the following applies when omitting the file pool ID and user ID from an SFS format profile name:
   a. If the file pool ID is omitted, RACF obtains the command issuer's default file pool ID, as follows:
      i) RACF uses the default file pool ID set by the SET FILEPOOL command, if SET FILEPOOL was used in the current CMS session to set a default file pool ID for this user.
      ii) RACF uses the file pool ID from the IPL of CMS, if SET FILEPOOL has not been used in the current CMS session to set a default file pool ID for this user. The file pool ID from the IPL could come from an explicitly issued IPL command or it could be from an IPL statement in the CP directory.
      iii) RACF uses a default file pool ID of NONE. In this case, the RACF command will fail with an error message.
   b. If the user ID is omitted, RACF obtains the command issuer's default file space, as follows:
      i) RACF uses the default file space set by the SET FILESPACE command, if SET FILESPACE was used in the current CMS session to set a default file space for this user.
      ii) RACF uses the command issuer's user ID, if SET FILESPACE has not been used to set a default file space for this user.
2. If a RACF SFS command is entered in a RACF command session on z/VM or the command is issued on z/OS, the following applies when omitting the file pool ID and user ID from an SFS format profile name:
   a. The file pool ID must be specified; otherwise, an error message will be issued.
   b. If the user ID qualifier is omitted from an SFS format profile name, the command issuer's user ID will be substituted for the user ID qualifier.

Table 15 on page 343 shows examples of these rules for specifying defaults in profile names for the FILE and DIRECTRY classes.

Table 15. Examples of default naming conventions

Name entered by user U	**Name used by RACF if SET FILEPOOL FP: was previously issued**	**Name used by RACF if SET FILEPOOL FP: and SET FILESPACE U2 were previously issued**
. **(*)**	FP:U.	FP:U2.
FP:U.	FP:U.	FP:U.
FP:.	FP:U.	FP:U2.
U. **(*)**	FP:U.	FP:U.
.U **(*)**	FP:U.U	FP:U2.U
FP:.SUBDIR1	FP:U.SUBDIR1	FP:U2.SUBDIR1
.SUBDIR1 **(*)**	FP:U.SUBDIR1	FP:U2.SUBDIR1

Table 15. Examples of default naming conventions (continued)		
Name entered by user U	**Name used by RACF if SET FILEPOOL FP: was previously issued**	**Name used by RACF if SET FILEPOOL FP: and SET FILESPACE U2 were previously issued**
U.SUBDIR1 **(*)**	FP:U.SUBDIR1	FP:U.SUBDIR1
FP:	not valid	not valid
FP:U	not valid	not valid
U	not valid	not valid
TEMP	not valid	not valid

(*) This name is not valid on z/OS and in the RACF command session on z/VM because the file pool qualifier is omitted.

Names for SFS Files

The format of SFS files follows SFS naming conventions. The format of a FILE name is:

```
   filename filetype directory-id
or
   filename filetype [file-pool-id:][userid].[dir1.dir2...dir8]
```

When using the SFS file commands (ADDFILE, ALTFILE, LFILE, DELFILE, PERMFILE and SRFILE), the profile name entered must be in SFS format, that is:

```
filename filetype file-pool-id:userid.dir1.dir2
```

To make authority checking more efficient, RACF converts the SFS format file name to a RACF format file name. The **RACF format** of SFS file names is:

```
file-pool-id.userid.dir1.dir2.filename.filetype
```

The RACF format must be used if defining an entry in the global access checking table. The RACF format is also used if entering RACF commands other than the RACF SFS file and directory commands, such as RLIST or SEARCH. We recommend using RACF SFS file commands where possible.

Discrete Profile:

A discrete profile name matches exactly the name of the SFS object it protects.

If the SFS file name is:

```
   ONE SCRIPT FP2:OPER.DIR1.DIR2
```

The discrete RACF profile name in SFS format is:

```
   ONE SCRIPT FP2:OPER.DIR1.DIR2
```

For example, this profile name can be used in the RACF SFS commands as follows:

```
ADDFILE ONE SCRIPT FP2:OPER.DIR1.DIR2 UACC(NONE) OWNER(ANDREW)

ADDDIR  FP2:OPER.DIR3 FCLASS(FILE) FROM(ONE SCRIPT FP2:OPER.DIR1.DIR2)

PERMFILE ONE SCRIPT FP2:OPER.DIR1.DIR2 ID(LAURIE) ACCESS(UPDATE)
```

Generic Profile:

The profile name of the file you specify can contain one or more generic characters (% , * or **) as described in the following section.

- Specify * to match zero or more characters at the end of a qualifier. If you specify a single asterisk as the only character in a qualifier, it represents one entire qualifier.

Note: An ending * in general resource classes **other** than FILE and DIRECTRY will match zero or more characters until the end of the resource name.

- Specify ** to match zero or more qualifiers in a resource name. You cannot specify any other characters with ** within a qualifier (for example, `FN FT FP:USER1.A**` is not allowed, but `FN FT FP:USER1.**` is).

  Note: ** cannot be used in the filename or filetype qualifiers in a file profile name. Only one occurrence of ** is allowed in a profile name.

- Specify % to match any single character in a resource name, including a generic character.

Note:

1. RACF does not allow you to specify any generic characters in the file pool ID or user ID qualifiers of the file profile name.
2. The ampersand (&) generic character can also be used in the FILE and DIRECTRY classes if the RACFVARS class is active. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

Generic Characters in SFS Names

Tables Table 16 on page 345, Table 17 on page 345, Table 18 on page 346, and Table 19 on page 346 show how you can use generic characters. In profile names for the FILE class, the first two qualifiers are required and always represent the file name and file type. The accompanying examples are for profiles in the FILE class, but generic characters are used in the DIRECTRY class in the same way.

Table 16. Using an Asterisk (*) as a Qualifier

Profile Name	**FN1 FT1 FP:U1.*.B**	**FN1 * FP:U1.A.B**	*** * FP:U1.A.B protects all files in U1's directory A.B**	*** * FP:USER1. protects all files in USER1's main directory**
Files Protected by the Profile	`FN1 FT1 FP:U1.A.B` `FN1 FT1 FP:U1.ABC.B`	`FN1 EXEC FP:U1.A.B` `FN1 LIST FP:U1.A.B`	`FN1 EXEC FP:U1.A.B` `FN2 LIST FP:U1.A.B`	`FN1 FT FP:USER1.`
Files Not Protected by the Profile	`FN1 FT1 FP:U1.X.Y.B` `FN1 FT1 FP:U1.B.X`	`FN1 FT1 FP:U1.A.B.C` `FN1 FT FP:U1.A.B.Z`	`FN1 FT1 FP:U1.A.B.C B` `FT FP:U1.A`	`FN1 FT1 FP:U1.A`

Table 17. Using an Asterisk (*) as the Last Character

Profile Name	**FW* FT1 FP:U1.A.B**	**FN FT FP:U1.A***
Files Protected by the Profile	`FW1 FT1 FP:U1.A.B` `FW123456 FT1 FP:U1.A.B`	`FN FT FP:U1.A123456` `FN FT FP:U1.A`
Files Not Protected by the Profile	`FW1 FT1 FP:U1.A.B.C`	`FN FT FP:U1.A1.B1`

Table 18. Using Two Asterisks (**) as a Qualifier				
Profile Name	*** * FP:U2.****	*** * FP:U1.A.****	*** EXEC FP:U1.A.B.****	*** * FP:U1.A.*.****
Files Protected by the Profile	L M FP:U2. FN FT FP:U2.A.B X Y FP:U2.A.B.C and all files belonging to U2 in filepool FP [1]	L M FP:U1.A FN FT FP:U1.A.B X Y FP:U1.A.B.C and all files in directory A and any of A's subdirectories [1]	LL EXEC FP:U1.A.B.C FN EXEC FP:U1.A.B and all EXEC files in B's directory and any of B's subdirectories [1]	FN FT FP:U1.A.B FN1 FT1 FP:U1.A.D F T FP:U1.A.B.C B EXEC FP:U1.A.ABC and all files in A's subdirectories [1]
Files Not Protected by the Profile	FN FT FP:USER2.	FN FT FP:U1.B	FN FT FP:U1.B B EXEC FP:U1.A.ABC	FN FT FP:U1.A and no files in directory A are protected [1]

Note:

1. This is only true if a more specific profile does not exist.

Table 19. Using a Percent Sign (%) in a Profile Name		
Profile Name	**F T FP:U1.A%CD**	*** * FP:U1.A%CD**
Files Protected by the Profile	F T FP:U1.ABCD F T FP:U1.AXCD	FN1 FT1 FP:U1.ABCD FILE1 TYPE1 FP:U1.AQCD
Files Not Protected by the Profile	FN FT FP:U1.ABBD	F T FP:U1.ABCC

Discrete and Generic Profiles

Regardless of whether a file profile is discrete or generic, RACF automatically grants full authority to the user whose user ID matches the user ID qualifier of the profile name.

Names for SFS Directories

The format of SFS directory names follows SFS naming conventions. The format of a DIRECTRY name is:

```
[file-pool-id:][userid].[dir1.dir2...dir8]
```

When using the RACF SFS directory commands (ADDDIR, ALTDIR, LDIRECT, DELDIR, PERMDIR and SRDIR), the profile name entered must be in SFS format, that is:

```
file-pool-id:user.dir1.dir2
```

To make authority checking more efficient, RACF converts the SFS format directory name to a RACF format directory name. The **RACF format** of SFS directory names is:

```
file-pool-id.user.dir1.dir2
```

The RACF format must be used if defining an entry in the global access checking table. The RACF format is used if entering RACF commands other than the RACF SFS file and directory commands, such as RLIST or SEARCH. We recommend using RACF SFS directory commands where possible.

Discrete Profile:

A discrete profile name matches exactly the name of the SFS object it protects.

If the SFS directory name is FP1:OPER.DIR1.DIR2.DIR3

The discrete RACF profile name in SFS format is `FP1:OPER.DIR1.DIR2.DIR3`

For example, this profile name can be used in the RACF SFS commands as follows:

```
ADDDIR FP1:OPER.DIR1.DIR2.DIR3 UACC(READ) SECLABEL(SECRET)

ADDFILE * * FP2:OPER.SAVE FCLASS(DIRECTRY) FROM(FP1:OPER.DIR1.DIR2.DIR3)

LDIRECT FP1:OPER.DIR1.DIR2.DIR3 STATISTICS AUTHUSER
```

Generic Profile:

The profile name you specify can contain one or more generic characters (% , * or **) as described in the following section.

- Specify % to match any single character in a resource name, including a generic character
- Specify * to match zero or more characters at the end of a qualifier. If you specify a single asterisk as the only character in a qualifier, it represents one entire qualifier.

  Note: An ending * in general resource classes **other** than FILE and DIRECTRY will match zero or more characters until the end of the resource name.
- Specify ** to match zero or more qualifiers in a resource name. You cannot specify any other characters with ** within a qualifier (for example, FP:USER1.A** is not allowed, but FP:USER1.** is).

Note:

1. RACF does not allow you to specify any generic characters in the file-pool-id or user ID qualifiers of the directory profile name.
2. The ampersand (&) generic character can also be used in the FILE and DIRECTRY classes if the RACFVARS class is active. For more information, see *z/VM: RACF Security Server Security Administrator's Guide*.

For examples of profile naming using these characters, see Table 17 on page 345 through Table 19 on page 346.

Discrete and Generic Profiles

Regardless of whether a directory profile is discrete or generic, RACF automatically grants full authority to the user whose user ID matches the user ID qualifier of the profile name.

Appendix B. IBM-Supplied Resource Classes that Apply to z/VM Systems

For a complete listing of all IBM-supplied resource classes in the CDT, see *z/VM: RACF Security Server Macros and Interfaces*.

Class	Purpose
DIRACC	Controls auditing (via SETROPTS LOGOPTIONS) for access checks for read/write access to HFS directories. Profiles are not allowed in this class.
DIRECTRY	Protection of shared file system (SFS) directories.
DIRSRCH	Controls auditing (via SETROPTS LOGOPTIONS) of HFS directory searches. Profiles are not allowed in this class.
FACILITY	Miscellaneous uses. Profiles are defined in this class so resource managers (typically program products or components) can check a user's access to the profiles when the users take some action. Examples are using combinations of options for tape mounts, and use of the RACROUTE interface. RACF does not document all of the resources used in the FACILITY class by other products. For information on the FACILITY-class resources used by a specific product (other than RACF itself), see that product's documentation.
FIELD	Fields in RACF profiles (field-level access checking).
FILE	Protection of shared file system (SFS) files.
FSOBJ	Controls auditing (via SETROPTS LOGOPTIONS) for all access checks for HFS objects except directory searches. Controls auditing (via SETROPTS AUDIT) of creation and deletion of HFS objects. Profiles are not allowed in this class.
FSSEC	Controls auditing (via SETROPTS LOGOPTIONS) for changes to the security data (FSP) for HFS objects. Profiles are not allowed in this class.
GLOBAL	Global access checking. [1]
GMBR	Member class for GLOBAL class (not for use on RACF commands).
GTERMINL	Terminals with IDs that do not fit into generic profile naming conventions. [1]
PROCESS	Controls auditing (via SETROPTS LOGOPTIONS) of changes to UIDs and GIDs of OpenExtensions VM processes. Controls auditing (via SETROPTS AUDIT) of dubbing and undubbing of OpenExtensions VM processes. Profiles are not allowed in this class.
PSFMPL	When class is active, PSF/VM performs separator and data page labeling as well as auditing.
PTKTDATA	PassTicket Key Class.
PTKTVAL	Used by NetView/Access Services Secured Single Signon to store information needed when generating a PassTicket.
RACFEVNT	RACFEVENT class contains profiles which control whether RACF change log notification is performed for USER profiles, and whether password or password phrase enveloping is to be performed.
RACFVARS	RACF variables. In this class, profile names, which start with & (ampersand), act as RACF variables that can be specified in profile names in other RACF general resource classes.

Class	Purpose
RVARSMBR	Member class for RACFVARS (not for use on RACF commands).
SCDMBR	Member class for SECDATA class (not for use on RACF commands).
SECDATA	Security classification of users and data (security levels and security categories). [1]
SECLABEL	If security labels are used and, if so, their definitions. [2]
SFSCMD	Controls the use of shared file system (SFS) administrator and operator commands.
SURROGAT	If surrogate submission is allowed, and if allowed, which user IDs can act as surrogates.
TAPEVOL	Tape volumes.
TERMINAL	Terminals (TSO or z/VM). See also GTERMINL class.
VMBATCH	Alternate user IDs.
VMCMD	CP commands, DIAGNOSE instructions, and system events.
VMDEV	Control who connects to real devices.
VMLAN	Use RACF to control Guest LANs
VMMAC	Used in conjunction with the SECLABEL class to provide security label authorization for some z/VM events. Profiles are not allowed in this class.
VMMDISK	z/VM minidisks.
VMNODE	RSCS nodes.
VMRDR	z/VM unit record devices (virtual reader, virtual printer, and virtual punch).
VMSEGMT	Restricted segments, which can be named saved segments (NSS) and discontiguous saved segments (DCSS).
VXMBR	Member class for VMXEVENT class (not for use on RACF commands).
VMXEVENT	Auditing and controlling security-related events (called z/VM events) on z/VM systems.
VMPOSIX	Contains profiles used by OpenExtensions z/VM.
WRITER	z/VM print devices.

Note:

1. You cannot specify this class name on the GENCMD, GENERIC, and GLOBAL/NOGLOBAL operands of the SETROPTS command.
2. You cannot specify this class name on the GLOBAL operand of the SETROPTS command or, if you do, the GLOBAL checking is not performed.

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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 grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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

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 jurisdictions 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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

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

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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.

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

This information may contain examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information may 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.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on IBM Copyright and trademark information (https://www.ibm.com/legal/copytrade).

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

Terms and Conditions for Product Documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal Use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

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

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

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

For more information about the use of various technologies, including cookies, for these purposes, see:

- The section entitled **IBM Websites** at IBM Privacy Statement (https://www.ibm.com/privacy)
- Cookies and Similar Technologies (https://www.ibm.com/privacy#Cookies_and_Similar_Technologies)

Bibliography

This topic lists the publications in the z/VM library. For abstracts of the z/VM publications, see *z/VM: General Information*.

Where to Get z/VM Information

The current z/VM product documentation is available in IBM Documentation - z/VM (https://www.ibm.com/docs/en/zvm).

z/VM Base Library

Overview

- *z/VM: License Information*, GI13-4377
- *z/VM: General Information*, GC24-6286

Installation, Migration, and Service

- *z/VM: Installation Guide*, GC24-6292
- *z/VM: Migration Guide*, GC24-6294
- *z/VM: Service Guide*, GC24-6325
- *z/VM: VMSES/E Introduction and Reference*, GC24-6336

Planning and Administration

- *z/VM: CMS File Pool Planning, Administration, and Operation*, SC24-6261
- *z/VM: CMS Planning and Administration*, SC24-6264
- *z/VM: Connectivity*, SC24-6267
- *z/VM: CP Planning and Administration*, SC24-6271
- *z/VM: Getting Started with Linux on IBM Z*, SC24-6287
- *z/VM: Group Control System*, SC24-6289
- *z/VM: I/O Configuration*, SC24-6291
- *z/VM: Running Guest Operating Systems*, SC24-6321
- *z/VM: Saved Segments Planning and Administration*, SC24-6322
- *z/VM: Secure Configuration Guide*, SC24-6323

Customization and Tuning

- *z/VM: CP Exit Customization*, SC24-6269
- *z/VM: Performance*, SC24-6301

Operation and Use

- *z/VM: CMS Commands and Utilities Reference*, SC24-6260
- *z/VM: CMS Primer*, SC24-6265
- *z/VM: CMS User's Guide*, SC24-6266
- *z/VM: CP Commands and Utilities Reference*, SC24-6268

- *z/VM: System Operation*, SC24-6326
- *z/VM: Virtual Machine Operation*, SC24-6334
- *z/VM: XEDIT Commands and Macros Reference*, SC24-6337
- *z/VM: XEDIT User's Guide*, SC24-6338

Application Programming

- *z/VM: CMS Application Development Guide*, SC24-6256
- *z/VM: CMS Application Development Guide for Assembler*, SC24-6257
- *z/VM: CMS Application Multitasking*, SC24-6258
- *z/VM: CMS Callable Services Reference*, SC24-6259
- *z/VM: CMS Macros and Functions Reference*, SC24-6262
- *z/VM: CMS Pipelines User's Guide and Reference*, SC24-6252
- *z/VM: CP Programming Services*, SC24-6272
- *z/VM: CPI Communications User's Guide*, SC24-6273
- *z/VM: ESA/XC Principles of Operation*, SC24-6285
- *z/VM: Language Environment User's Guide*, SC24-6293
- *z/VM: OpenExtensions Advanced Application Programming Tools*, SC24-6295
- *z/VM: OpenExtensions Callable Services Reference*, SC24-6296
- *z/VM: OpenExtensions Commands Reference*, SC24-6297
- *z/VM: OpenExtensions POSIX Conformance Document*, GC24-6298
- *z/VM: OpenExtensions User's Guide*, SC24-6299
- *z/VM: Program Management Binder for CMS*, SC24-6304
- *z/VM: Reusable Server Kernel Programmer's Guide and Reference*, SC24-6313
- *z/VM: REXX/VM Reference*, SC24-6314
- *z/VM: REXX/VM User's Guide*, SC24-6315
- *z/VM: Systems Management Application Programming*, SC24-6327
- *z/VM: z/Architecture Extended Configuration (z/XC) Principles of Operation*, SC27-4940

Diagnosis

- *z/VM: CMS and REXX/VM Messages and Codes*, GC24-6255
- *z/VM: CP Messages and Codes*, GC24-6270
- *z/VM: Diagnosis Guide*, GC24-6280
- *z/VM: Dump Viewing Facility*, GC24-6284
- *z/VM: Other Components Messages and Codes*, GC24-6300
- *z/VM: VM Dump Tool*, GC24-6335

z/VM Facilities and Features

Data Facility Storage Management Subsystem for z/VM

- *z/VM: DFSMS/VM Customization*, SC24-6274
- *z/VM: DFSMS/VM Diagnosis Guide*, GC24-6275
- *z/VM: DFSMS/VM Messages and Codes*, GC24-6276
- *z/VM: DFSMS/VM Planning Guide*, SC24-6277

- *z/VM: DFSMS/VM Removable Media Services*, SC24-6278
- *z/VM: DFSMS/VM Storage Administration*, SC24-6279

Directory Maintenance Facility for z/VM

- *z/VM: Directory Maintenance Facility Commands Reference*, SC24-6281
- *z/VM: Directory Maintenance Facility Messages*, GC24-6282
- *z/VM: Directory Maintenance Facility Tailoring and Administration Guide*, SC24-6283

Open Systems Adapter

- Open Systems Adapter/Support Facility on the Hardware Management Console (https://www.ibm.com/docs/en/SSLTBW_2.3.0/pdf/SC14-7580-02.pdf), SC14-7580
- Open Systems Adapter-Express ICC 3215 Support (https://www.ibm.com/docs/en/zos/2.3.0?topic=osa-icc-3215-support), SA23-2247
- Open Systems Adapter Integrated Console Controller User's Guide (https://www.ibm.com/docs/en/SSLTBW_2.3.0/pdf/SC27-9003-02.pdf), SC27-9003
- Open Systems Adapter-Express Customer's Guide and Reference (https://www.ibm.com/docs/en/SSLTBW_2.3.0/pdf/ioa2z1f0.pdf), SA22-7935

Performance Toolkit for z/VM

- *z/VM: Performance Toolkit Guide*, SC24-6302
- *z/VM: Performance Toolkit Reference*, SC24-6303

The following publications contain sections that provide information about z/VM Performance Data Pump, which is licensed with Performance Toolkit for z/VM.

- *z/VM: Performance*, SC24-6301. See z/VM Performance Data Pump.
- *z/VM: Other Components Messages and Codes*, GC24-6300. See Data Pump Messages.

RACF Security Server for z/VM

- *z/VM: RACF Security Server Auditor's Guide*, SC24-6305
- *z/VM: RACF Security Server Command Language Reference*, SC24-6306
- *z/VM: RACF Security Server Diagnosis Guide*, GC24-6307
- *z/VM: RACF Security Server General User's Guide*, SC24-6308
- *z/VM: RACF Security Server Macros and Interfaces*, SC24-6309
- *z/VM: RACF Security Server Messages and Codes*, GC24-6310
- *z/VM: RACF Security Server Security Administrator's Guide*, SC24-6311
- *z/VM: RACF Security Server System Programmer's Guide*, SC24-6312
- *z/VM: Security Server RACROUTE Macro Reference*, SC24-6324

Remote Spooling Communications Subsystem Networking for z/VM

- *z/VM: RSCS Networking Diagnosis*, GC24-6316
- *z/VM: RSCS Networking Exit Customization*, SC24-6317
- *z/VM: RSCS Networking Messages and Codes*, GC24-6318
- *z/VM: RSCS Networking Operation and Use*, SC24-6319
- *z/VM: RSCS Networking Planning and Configuration*, SC24-6320

TCP/IP for z/VM

- *z/VM: TCP/IP Diagnosis Guide*, GC24-6328
- *z/VM: TCP/IP LDAP Administration Guide*, SC24-6329
- *z/VM: TCP/IP Messages and Codes*, GC24-6330
- *z/VM: TCP/IP Planning and Customization*, SC24-6331
- *z/VM: TCP/IP Programmer's Reference*, SC24-6332
- *z/VM: TCP/IP User's Guide*, SC24-6333

Prerequisite Products

Device Support Facilities

- Device Support Facilities (ICKDSF): User's Guide and Reference (https://www.ibm.com/docs/en/SSLTBW_2.5.0/pdf/ickug00_v2r5.pdf), GC35-0033

Environmental Record Editing and Printing Program

- Environmental Record Editing and Printing Program (EREP): Reference (https://www.ibm.com/docs/en/SSLTBW_2.5.0/pdf/ifc2000_v2r5.pdf), GC35-0152
- Environmental Record Editing and Printing Program (EREP): User's Guide (https://www.ibm.com/docs/en/SSLTBW_2.5.0/pdf/ifc1000_v2r5.pdf), GC35-0151

Related Products

XL C++ for z/VM

- *XL C/C++ for z/VM: Runtime Library Reference*, SC09-7624
- *XL C/C++ for z/VM: User's Guide*, SC09-7625

z/OS

IBM Documentation - z/OS (https://www.ibm.com/docs/en/zos)

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z

Product Number: 5741-A09

Printed in USA

SC24-6306-73