z/VM

RACF Security Server General User's Guide

Version 6 Release 3

SC24-6215-01

Note:
Before using this information and the product it supports, read the information in "Notices" on page 87.

This edition applies to version 6, release 3, modification 0 of IBM z/VM (product number 5741-A07) and to all subsequent releases of this product until otherwise indicated in new editions.

This edition replaces SC24-6215-00.

Contents

Figures

Tables

About This Document

This document teaches the general user how to use the IBM® RACF® Security Server for z/VM® to perform security functions. It contains an introduction to RACF, as well as sections that guide the user through basic security tasks on z/VM.

Who Should Read This Document

This document is for:

- General users who need to use RACF to protect their own minidisks, SFS files, SFS directories, or other general resources
- Users responsible for the security of a group minidisk.

You can use panels or commands to perform these tasks.

What You Should Know Before Reading This Document

Before you use this document, you should:

- Know how to conduct a conversational monitor system (CMS) terminal session
- Know how to enter commands or use interactive system productivity facility (ISPF) panels
- Be defined to RACF.

To find out how to use CMS, see the *z/VM: CMS Primer*

How to Use This Document

To use this document:

1. Read Chapter 1, "What Is RACF?," on page 1. It tells you how RACF provides security on the operating system and protects your resources.

   Chapters 2 through 7 contain step-by-step procedures for you to follow. You don't need to have any previous experience with RACF to go through them.
2. Choose whether you want to use the RACF panels or commands to perform the security tasks you want to do.
   a. If you want to use panels, read Chapter 2, "Using RACF Panels," on page 5. This chapter explains how to get help while using the RACF panels.
   b. The rest of this document shows you how to use RACF commands. "RACF Commands for General User Tasks" on page 7 contains tables that list which commands to use to perform your security tasks.

Where to Find More Information

For information about related publications, refer to the "Bibliography" on page 93.

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 Send Your Comments to IBM

We appreciate your input on this publication. Feel free to comment on the clarity, accuracy, and completeness of the information or give us any other feedback that you might have.

Use one of the following methods to send us your comments:

1. Send an email to mhvrcfs@us.ibm.com.
2. Go to IBM z/VM Reader's Comments (www.ibm.com/systems/z/os/zvm/zvmforms/webqs.html).

Include the following information:

- Your name
- Your email address
- The publication title and order number:
  z/VM V6.3 RACF Security Server General User's Guide
  SC24-6215-01
- The topic name or page number related to your comment
- The text of your comment

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

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

If You Have a Technical Problem

Do not use the feedback methods listed above. Instead, do one of the following:

- Contact your IBM service representative.
- Contact IBM technical support.
- See IBM: z/VM Service Resources (www.ibm.com/vm/service/).
- Go to IBM Support Portal (www.ibm.com/support/entry/portal/Overview/).

Summary of Changes

This document contains terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change. Some program updates might be provided through z/VM service by program temporary fixes (PTFs) for authorized program analysis reports (APARs), which also might be available for some prior releases.

All z/OS-specific information has been removed from this library. Remaining z/OS® information either pertains to both platforms or has other relevance to z/VM.

SC24-6215-01, z/VM Version 6 Release 3 (September 2015)

This edition includes changes to support product changes provided or announced after the general availability of z/VM V6.3.

SC24-6215-00, z/VM Version 6 Release 1

This edition supports the general availability of z/VM V6.1.

Chapter 1. What Is RACF?

Resource Access Control Facility (RACF) is a software security product that protects information by controlling access to it. RACF also controls what you can do on the operating system and protects your resources. It provides this security by identifying and verifying users, authorizing users to access protected resources, and recording and reporting access attempts.

Identifying and Verifying Users

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

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

Note: Some applications may not support password phrases. For these applications, you must use your password.

When you are first defined to RACF, your group or security administrator assigns you a user ID and a temporary password. This temporary password enables you to log on to the system the first time. As soon as you log on, RACF requires you to supply a new password of your choice. Your password may expire after a certain time interval; so you may have to change it periodically. See “Changing Your Password” on page 26 for more information.

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

You might also be assigned a password phrase. If so, the first time you log on, RACF requires you to supply a new password phrase of your choice. Your password phrase might expire after a certain time interval, so you might need to change it periodically. See “Using the PASSWORD Command” on page 26 for more information.

Giving Users Access to Protected Resources

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

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

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

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

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

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

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

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

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

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

person to the access list with the authority to view, but not change, your data. In this way, RACF helps you protect your work.

Recording and Reporting Access Attempts

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

Chapter 2. Using RACF Panels

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

```
ISPF
```

or:

```
RACF (PANEL
```

If you enter **ISPF**, the ISPF primary menu appears. Choose option **R** for RACF.

Note:

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

You will see the following RACF menu:

```
                        RACF - SERVICES OPTION MENU
OPTION ===>

SELECT ONE OF THE FOLLOWING:

   1  DATA SET PROFILES

   2  GENERAL RESOURCE PROFILES
   3  GROUP PROFILES AND USER-TO-GROUP CONNECTIONS
   4  USER PROFILES AND YOUR OWN PASSWORD
   5  SYSTEM OPTIONS

   6  VM DUAL REGISTRATION
   7  VM EVENTS
   8  VM MINIDISK PROFILES
   9  VM FILE PROFILES
  10  VM DIRECTORY PROFILES

  98  TUTORIAL
  99  EXIT
```

From here, you can get to menus of different tasks you might need to do with RACF. These menus lead you through the panels, providing options that let you:

- Find out what authority you have
- Protect a minidisk, an SFS file, or an SFS directory
- Change your password or password phrase

To get more information about a particular panel, type **help** on the command line or press the PF1 key.

You may need to know a panel ID for diagnosis. To display the panel ID in the upper left part of the screen, enter:

```
panelid
```

to the right of `OPTION ===>`, as follows:

```
                        RACF - SERVICES OPTION MENU
OPTION ===> panelid
```

To choose the tutorial option from the menu, enter:

98

to the right of OPTION ===>, as follows:

```
                        RACF - SERVICES OPTION MENU
OPTION ===> 98
```

You will see the following tutorial menu:

```
TUTORIAL                        RACF Tutorial
Option ===>

         To view the following topics in sequence, press ENTER.
         For a specific topic, enter the number of your selection.

          1  About this Tutorial
          2  RACF Concepts
          3  Using RACF on MVS
          4  Using RACF on VM









      ENTER = Proceed                       PF03 = End tutorial
```

With this tutorial, you can learn how to use the RACF panels to perform your security tasks. Each option on the tutorial panel gives you definitions for user IDs and passwords, user and group profiles, resource profiles, authorities, and attributes.

Chapter 3. Using RACF Commands

You can use RACF commands to perform security tasks. RACF commands enable you to find out how you are defined to RACF, to protect your resources, to change another user's access to your resources, and to change how RACF defines you.

You can enter RACF commands by the methods described in "Using the RAC Command" on page 10, "Using a RACF Command Session" on page 11, or Appendix F, "Using RACFISPF," on page 85.

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

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

RACF Commands for General User Tasks

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

For information about how to handle security for your OpenExtensions files and directories, see *z/VM: OpenExtensions User's Guide* or

Table 1. RACF Commands for General User Tasks

Task	Command
"Finding Out How You Are Defined to RACF" on page 14	`rac listuser`
"Logging on with a Security Label" on page 23	`logon` *`userid`* `seclabel` *`security-label`* **Note:** LOGON is a z/VM command.
"Logging On To Shared User IDs" on page 24s	`logon` *`shared-userid`* `by` *`surrogate-userid`*
"Changing Your Password" on page 26	`rac password` ` password(`*`current-password new-password`*`)`

"Changing your Password Phrase" on page 28	`rac password`
	` phrase(`*`current-password-phrase new-password-phrase`*`)`
	
	or
	`rac phrase`
	` phrase(`*`current-password-phrase new-password-phrase`*`)`

Table 1. RACF Commands for General User Tasks (continued)

Task	Command

"Changing Your Password Interval" on page 27	`rac password interval(nnn)`
	
	or
	`rac phrase interval(nnn)`

"Changing Your Default Group" on page 30	`rac altuser dfltgrp(group-name)`

Table 2. RACF Commands for Minidisk Tasks

Task	Command
"Finding Out About Your Minidisk Profiles" on page 31	`rac search class(vmmdisk) mask(userid)`
"Finding Out How a Minidisk Is Protected" on page 32	`rac rlist vmmdisk userid.virtual-address all`
"Changing the Universal Access Authority to a Minidisk" on page 38	`rac ralter vmmdisk profile-name uacc(access-authority)`
"Permitting an Individual or a Group to Use a Minidisk" on page 39	`rac permit profile-name class(vmmdisk) id( userid|groupid) access(level)`

"Denying an Individual or a Group Use of a Minidisk" on page 41	`rac permit profile-name class(vmmdisk) id( userid|groupid) access(none)`
	
	or
	`rac permit profile-name class(vmmdisk) id(userid|groupid) delete`

Table 3. RACF Commands for SFS File Tasks

Task	Command
"Get a List of SFS File Profiles" on page 45	`rac srfile`
"Add a Profile for an SFS File" on page 46	`rac addfile profile-name`
"List Information in an SFS File Profile" on page 46	`rac lfile file-name`
"Change a Profile for an SFS File" on page 48	`rac altfile profile-name`
"Maintain SFS File Access Lists" on page 49	`rac permfile profile-name id(userid|groupid) access(access-authority)`
"Delete a Profile for an SFS File" on page 49	`rac delfile profile-name`

Table 4. RACF Commands for SFS Directory Tasks

Task	Command
"Get a List of SFS Directory Profiles" on page 49	`rac srdir`

Table 4. RACF Commands for SFS Directory Tasks (continued)

Task	Command
"Add a Profile for an SFS Directory" on page 50	`rac adddir profile-name`
"List Information in an SFS Directory Profile" on page 51	`rac ldirect directory-name`
"Change a Profile for an SFS Directory" on page 53	`rac altdir profile-name`
"Maintain SFS Directory Access Lists" on page 54	`rac permdir profile-name id(userid|groupid) access(access-authority)`
"Delete a Profile for an SFS Directory" on page 54	`rac deldir profile-name`

Table 5. RACF Commands for General Resource Tasks

Task	Command
"Searching for General Resource Profile Names" on page 56	`rac search class(class-name)`
"Listing the Contents of General Resource Profiles" on page 57	`rac rlist class-name profile-name`
"Permitting an Individual or a Group to Use a General Resource" on page 58	`rac permit profile-name class(class-name) id(userid|groupid) access(access-authority)`

"Denying an Individual or a Group Use of a General Resource" on page 58	`rac permit profile-name class(class-name) id(userid|groupid) access(none)`
	or
	`rac permit profile-name class(class-name) id(userid|groupid) delete`

Online Help for RACF Commands

To get online help for a RACF command, type:

```
rac help command-name
```

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

```
rac help permit
```

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

```
rac help command-name syntax
```

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

```
rac help permit syntax
```

Note: These examples use the RAC command form of the HELP command. To use these commands in a RACF command session, omit rac at the beginning of the command.

Escaping From a Command Prompt Sequence

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

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 to exit.

Using the RAC Command

To enter RACF commands without isolating yourself in a RACF command session, use the RAC command. You can continue to enter CP or CMS commands from line mode or FILELIST menus.

To enter RACF commands during a z/VM terminal session, use the following syntax:

```
rac racf-command
```

If your installation has restricted access to the RAC command, you may not be able to use the RAC command shown here. In that case, ask your security administrator for access to the RAC command.

When you use RAC, output from the most recent RACF command entered is written to the RACF DATA file and the command output is displayed to your terminal screen. The next RACF command you issue overwrites the RACF DATA file.

If you do not want the command output to be displayed to your terminal, enter the CMS command:

```
globalv select $racgrp set $rac_ispf y
```

If you do not want subsequent commands to overwrite the RACF DATA file, you can append the file (send the output you enter from all RACF commands you enter to the file) by entering the CMS command:

```
globalv select $racgrp set $rac_apn y
```

If you choose to have your output appended, the output is not displayed to your terminal.

The RACF DATA file defaults to your disk or directory accessed as A unless specified otherwise by your installation. If you cannot find the file on your disk or directory accessed as A, check your other disks or directories. If you would like to have the output placed on your disk or directory accessed as B, enter the CMS command:

```
globalv select $racgrp set $rac_fle b
```

Note: You must have write access to the output disk or directory. Otherwise, an error will occur and you won't see the desired output.

For more information about changing RAC command defaults, see *z/VM: RACF Security Server Command Language Reference*

Using a RACF Command Session

Attention

RACF command sessions may have restricted usage. It is recommended that general users enter RACF commands with the RAC command. If you need to enter a RACF command session, contact your security administrator.

You can enter RACF commands during a z/VM terminal session by entering a RACF command session. To begin a RACF command session, enter:

```
racf
```

Notes:

1. RACF does not require that you enter a password or password phrase to establish a RACF command session. However, your installation may. If your installation requires a password, RACF prompts you for your logon password. After you have entered your password, you can enter valid RACF z/VM commands. If you have a password phrase, you can enter that instead of your password. Do not enclose your password phrase in quotes when entering it at the prompt.

   If you choose to change your password or password phrase at this time, and are then denied access because your installation has restricted usage of the RACF command session, your password or password phrase change is still in effect.
2. When you are in a RACF command session, you can issue only valid RACF commands. Commands such as CP or CMS commands are not valid in a RACF command session, even though they are valid on VM.

   For information on what to do if you make a mistake entering a RACF command in a RACF command session, see "Escaping From a Command Prompt Sequence" on page 10.
3. You cannot issue RVARY, SETROPTS, or SETEVENT command from a RACF command session running on any system in an SSI cluster. In an SSI cluster, these commands must be entered using the RAC command.

To end a RACF command session at any time, enter:

```
end
```

For more information on RACF command sessions, see *z/VM: RACF Security Server Command Language Reference*

Chapter 4. RACF and You

To use the computer system, you must be defined to RACF. RACF records security information about you in a user profile. The profile contains information such as when you last updated your password, what group you belong to, and what individual and group authority you have on the system. Using this profile, RACF protects the system and the resources on the system. RACF lets you use the resources you have authority to access.

Finding Out If You Are Defined to RACF

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

If RACF is installed on your z/VM system and you can log on, you are RACF-defined. Log on to the system by entering your user ID. If you do not know if you have a user ID, see your group or security administrator or someone in authority at your installation. Without a user ID, you cannot use the system.

Note: If this is the first time you have ever logged on to the system, you must change your password. After you have entered your assigned temporary password, you will receive a message saying that it has expired. Enter a new password of your choice, following the password rules set by your installation. See “Changing Your Password” on page 26 to change your password.

Finding Out How You Are Defined to RACF

RACF builds a description of you and your authority in a user profile. Each RACF-defined user has a user profile containing information about his or her identity, user attributes, group, and password. You belong to at least one group. This group is a default group that your security administrator has assigned you to. RACF has defined a profile for this group. This profile contains information about the group, its members, and the authority its members have to use the group's resources.

To see how you are defined to RACF, enter:

```
rac listuser your-userid
```

You see output similar to that shown in Figure 1 on page 15. The sections "Understanding How You Are Defined to RACF" on page 15 and "Finding Out Your Authority as a Group Member" on page 18 describe what this RACF information means.

Note: The output of the LISTUSER command is shown as it should appear on your screen. Profile data for both the user and for the groups to which the user is connected is displayed.

```
USER=your   NAME=your name      OWNER=the owner   CREATED=date you were
     userid                           of this profile     defined to RACF

 DEFAULT-GROUP=     PASSDATE=            PASS-INTERVAL=       PHRASEDATE=
 your               date your            length of time       date your
 default            password was         your password        password phrase was
 group name         last updated         is valid             last updated

 PASSWORD ENVELOPED=password envelope status

 PHRASE ENVELOPED=password phrase envelope status

 ATTRIBUTES=your operating privileges and restrictions

 REVOKE DATE=date on which      RESUME DATE=date on which RACF allows
            RACF prevents you             you to use the system
            from using the system         again

 LAST-ACCESS=last date you used the system

 CLASS AUTHORIZATIONS=installation-assigned classes in which you
                      can define profiles.

 INSTALLATION-DATA=information your installation maintains about you

 MODEL-NAME=a profile used as a model for new data set profiles

 LOGON ALLOWED   (DAYS)           (TIME)

------------------------------------------------------------------

 days access is allowed           time access is allowed


  GROUP=name  AUTH=your  CONNECT-OWNER=owner   CONNECT-DATE=date you
        of         group             of this              were connected
        group      authority           group              to this group

    CONNECTS=number of times   UACC=universal    LAST-CONNECT=last time
          you were connected        access                    you were
               to this group        authority                 connected

    CONNECT ATTRIBUTES=your operating privileges as a member of this group

    REVOKE DATE=date on which      RESUME DATE=date on which RACF
                RACF prevents you             allows you to access
                from accessing the system     the system again
                through this group            through this group


SECURITY-LEVEL=your installation-assigned security level
CATEGORY-AUTHORIZATION=your installation-assigned security categories
SECURITY-LABEL=your installation-assigned security label
```

Figure 1. Output of the LISTUSER Command on z/VM

Understanding How You Are Defined to RACF

The following terms appear in the first part of the screen shown in Figure 1 after the LISTUSER command is entered. This information refers to RACF information about you, the user.

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

NAME
Your name as recorded in your user profile.

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

CREATED
The date you were defined to RACF.

DEFAULT-GROUP
RACF connects each user to at least one group. If you are connected to only one group, that group is your default group and that group name appears in this field. If you are a member of more than one group, you can change this field in your user profile (using the ALTUSER command). See "Changing Your Default Group" on page 30 for more information. When you log on again, the new group is your current connect group.

PASSDATE
The date you last updated your password or N/A if you do not have a password. A special value of 00.000 indicates that your password is expired, and must be changed when you next log on.

PASS-INTERVAL
The length of time in days your current password is valid. You must change your password before this interval expires.

PHRASEDATE
The date you last updated your password phrase, or N/A if you do not have a password phrase. A special value of 00.000 indicates that your password phrase is expired, and must be changed when you next log on.

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

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

ATTRIBUTES
The operating privileges and restrictions assigned to you as a user.

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

NOPASSWORD
Indicates that you do not have a password. You must log on to the system using a password phrase.

PASSPHRASE
Indicates that you have been assigned a password phrase.

SPECIAL
Allows full authorization to all profiles in the RACF data base and allows you to perform all RACF functions except those requiring the AUDITOR attribute.

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

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

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

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

REVOKE DATE
This term appears at least twice in the output. On the user part of the output, this is the date on which RACF begins preventing you from using the system. On each group part of the output, this is the date on which RACF begins preventing you from using the system when you try to connect to this group.

RESUME DATE
This term appears at least twice in the output. In the user part of the output, this is the date on which RACF allows you to resume using the system. In each group part of the output, this is the date on which RACF allows you to resume using the system when you are connected to this group.

LAST-ACCESS
This date is the last time you accessed the system. RACF keeps records of all persons who have accessed the system, and what they have done, as well as recording unauthorized attempts to access the system.

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

INSTALLATION-DATA
Additional information your installation maintains about you and your authority. If you need help to understand anything included here, see your RACF security administrator or the owner of your user profile.

MODEL-NAME
A profile used as a model for new resource profiles. (This term applies to z/OS systems only, and only has meaning if the RACF database is being shared with a z/OS system.)

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

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

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

SECURITY-LABEL
Your installation can define various security labels. A security label is a name used to represent the association between a particular security level and certain security categories. The name appearing in this field is the default security label assigned to you.

Note: Your current security label may differ from your default security label; to determine which security label is active for your user ID, enter `RACSEC`. (For more information on how to use the RACSEC EXEC, refer to "Displaying Your Security Label" on page 22.)

Finding Out Your Authority as a Group Member

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

When you log on, RACF connects you to your default group. If you wish to connect to a group other than your default group, you can change the default group field in your user profile (using the ALTUSER command). See "Changing Your Default Group" on page 30 for information on how to do this. When you are connected to a group, RACF allows you privileges within the group.

Displaying Your User Attributes

To see how you are defined to RACF, enter the LISTUSER command:

```
rac listuser
```

You see output similar to that shown in Figure 1 on page 15. The information in the second part of the screen shown in Figure 1 on page 15 describes the RACF group or groups you belong to and what you can do as a member of that group. This information refers to RACF information about the group you belong to and the authority you have as a member of that group.

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

GROUP
The name of the group to which you are connected.

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

USE Allows you to enter the system under the control of the specified group. You may use any of the resources the group may use.

CREATE
On z/OS systems, allows you to RACF-protect group resources and control who can access them. It includes the privileges of the USE authority.

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

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

CONNECT-OWNER
The owner of this group.

CONNECT-DATE
The date you were first connected to this group.

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

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

The UACC can be one of the following: NONE, READ, UPDATE, CONTROL, or ALTER. For descriptions of these values, see "Access Authority for Minidisks on z/VM" on page 71 and "Access Authority for General Resources" on page 73.

Attention

Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected resource can create a copy of it. As owner of the copied resource, that user has control of the security characteristics of the copied resource, and can downgrade it. For this reason, you may want to initially assign a UACC of NONE, and then selectively permit a small number of users to access your resource, as their needs become known. (For information on how to permit selected users or groups to access a resource, see "Permitting an Individual or a Group to Use a Minidisk" on page 39 or "Permitting an Individual or a Group to Use a General Resource" on page 58.)

LAST-CONNECT
The last time you were connected to the group.

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

NONE

SPECIAL

AUDITOR
OPERATIONS
REVOKE

For a description of each of these attributes, see the ATTRIBUTES field on page "ATTRIBUTES " on page 16.

REVOKE DATE
This term appears twice in the output. In the user portion of the output, this is the date on which RACF begins preventing you from using the system. In the group portion of the output, this is the date on which RACF begins preventing you from using the system when you try to connect to the group.

RESUME DATE
This term appears twice in the output. In the user portion of the output, this is the date on which RACF allows you to resume using the system. In the group portion of the output, this is the date on which RACF allows you to resume using the system when you are connected to this group.

The LISTUSER Command: Sample Output

Example 1:

A.H. Lee is an employee in the payroll department. A.H. Lee has a user ID of AHLEE. If he entered the LISTUSER command, he would see output similar to that shown in Figure 2. He would see information about how he is defined to RACF and information about the group or groups he belongs to.

```
USER=AHLEE  NAME=A.H.LEE               OWNER=JONES     CREATED=06.321
 DEFAULT-GROUP=PAYROLL  PASSDATE=06.321 PASS-INTERVAL= 30 PHRASEDATE=06.321
 ATTRIBUTES=PASSPHRASE
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=06.321/13:47:45
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
 LOGON ALLOWED   (DAYS)          (TIME)
 -----------------------------------------
 ANYDAY                          ANYTIME
  GROUP=PAYROLL   AUTH=USE      CONNECT-OWNER=OPERATOR  CONNECT-DATE=06.321
    CONNECTS=    00  UACC=NONE     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 2. LISTUSER Command Output: Example 1

In the example, user A.H. Lee is connected to only one group, PAYROLL. He has none of the privileged user attributes, but can still use RACF. For example, Lee can create, change, and delete RACF profiles to protect his resources. Lee has a password phrase, in addition to a password.

Example 2:

J.E. Smith is an employee in the auditing department. J.E. Smith has a user ID of SMITH. If she entered the LISTUSER command, she would see output similar to

that shown in Figure 3. She would see information about how she is defined to RACF and information about the group or groups she belongs to.

```
USER=SMITH   NAME=J.E.SMITH   OWNER=JONES  CREATED=88.096

 DEFAULT-GROUP=SEARCH  PASSDATE=N/A  PASS-INTERVAL= 30 PHRASEDATE=07.052

 ATTRIBUTES=NOPASSWORD PASSPHRASE AUDITOR

 REVOKE DATE=NONE   RESUME DATE=NONE

 LAST-ACCESS=90.114/13:47:18

 CLASS AUTHORIZATIONS=NONE

 NO-INSTALLATION-DATA

 NO-MODEL-NAME

 LOGON ALLOWED   (DAYS)           (TIME)

---------------------------------------------------------------

 ANYDAY                           ANYTIME

  GROUP=SEARCH AUTH=JOIN CONNECT-OWNER=WILL CONNECT-DATE=88.096

    CONNECTS= 01   UACC=NONE   LAST-CONNECT=90.114/13:50:18

    CONNECT ATTRIBUTES=NONE

    REVOKE DATE=NONE   RESUME DATE=NONE

  GROUP=PAYROLL AUTH=CREATE CONNECT-OWNER=MILL CONNECT-DATE=88.096

    CONNECTS= 00  UACC=READ  LAST-CONNECT=90.114/13:55:18

    CONNECT ATTRIBUTES=NONE

    REVOKE DATE=NONE   RESUME DATE=NONE

SECURITY-LEVEL=NONE SPECIFIED

CATEGORY-AUTHORIZATION
 NONE SPECIFIED

SECURITY-LABEL=NONE SPECIFIED
```

Figure 3. LISTUSER Command Output: Example 2

In the example, SMITH has been assigned a password phrase, but not a password.

Smith is connected to two groups, SEARCH and PAYROLL. She has the AUDITOR system-wide attribute. Not only can Smith control access to her resources, but as system AUDITOR, she can audit security controls and create security reports.

Smith's default group is the SEARCH group. She is automatically connected to that group when she logs on. In the SEARCH group, Smith has JOIN group authority and can assign group authorities to members of the group. In the PAYROLL group, Smith has CREATE group authority and can create resource profiles to protect group resources.

In the PAYROLL group, Smith also has assigned a UACC (universal access authority) of READ. Smith can connect to the PAYROLL group by changing the

default group field in her user profile to PAYROLL (using the ALTUSER command). When she logged on again she would be connected to that group. If PAYROLL is Smith's current connect group, any resource profiles she creates have a UACC of READ (unless she specifies otherwise).

Displaying Your Security Label

To determine the current security label for your user ID, enter:

```
racsec
```

If a SECLABEL is defined for your user ID, the following message is displayed:

```
RACSEC004I  The security label for user userid is seclabel.
```

If you do not have a SECLABEL defined for your user ID, the following message is displayed:

```
RACSEC002I  Userid userid is not currently logged on, or does
            not have a security label.
```

Finding Out Your OpenExtensions Information

Your user profile may contain OpenExtensions information about you, in the OVM segment.

RACF lists these details from the OVM segment of your user profile:

- User identifier (UID)
- Initial directory path name (HOME)
- Program path name (PROGRAM)
- File system root (FSROOT)

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

```
USER=your-user-ID

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

Figure 4. OVM Information in LISTUSER Command Output: Description

Note:

1. If there is no information in a field in the user's profile for this segment, the field name is not displayed. However, if UID was not specified when the OVM segment was added to the user profile, the word NONE appears in the listing.
2. The ability to view and update OVM information can be controlled on a field by field basis; therefore, any individual field may not appear on your output.

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

```
listuser your-userid ovm noracf
```

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

```
USER=CSMITH

OVM INFORMATION
---------------
 UID= 0000000024
 HOME= /u/CSMITH
 PROGRAM= /u/CSMITH/bin/myshell
 FSROOT= /../VMBFS:FILEPOOL:CSMITH/
```

Figure 5. OVM Information in LISTUSER Command Output: Example 1

If there is no value for HOME, PROGRAM, or FSROOT in the OVM segment of your profile, you see output similar to this:

```
USER=CSMITH

OVM INFORMATION
---------------
 UID= 0000000024
```

Figure 6. OVM Information in LISTUSER Command Output: Example 2

Your security administrator might have defined the OVM information so that you are able to alter certain fields. If so, and you want to change your current working directory, use the ALTUSER command as follows:

`altuser` *`your-userid`* `ovm(home(`*`your-new-current-working-directory`*`))`

This change will not take effect until the next time you log on.

See *z/VM: RACF Security Server Command Language Reference* for information about the ALTUSER command.

Logging on with a Security Label

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

A *security label* is used to represent the association between a particular security level and a set of 0 or more security categories. For example, the security categories PAYROLL and PERSONNEL may both be associated with the security level SECRET by the security label PPSECR.

If your installation uses security classifications, RACF lists the security classifications for each user and each resource in user and resource profiles. When you request access to a resource, RACF checks your user profile and the resource profile to see if your security label gives you access to the resource. RACF denies you access if you do not have the appropriate level.

Your security administrator defines a default security label for you. However you may be able to log on with a different security label if you have been authorized. This security label allows you to access resources that are available to you at that security label.

Note: Your installation must have the security label (SECLABEL) class active to log on with a security label. Ask your security administrator.

To log on with a security label other than your default security label:

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

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

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

   To see this list, enter:

   ```
   rac search class(seclabel)
   ```

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

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

   ```
   logon userid seclabel security-label
   ```

   The *userid* is your user ID and the *security-label* is the name of the security label you want to log on with. This security label will be in effect for the duration of the logon session.

   For example, suppose your user ID is WAYNE. To log on with the security label XFILES, enter:

   ```
   logon wayne seclabel xfiles
   ```

   The security label XFILES will be in effect for the duration of the logon session.

Logging On To Shared User IDs

With the RACF LOGON BY function, multiple users can share the same user ID. Only one user can be logged on to the shared user ID at any given time.

You can log on to a shared user ID by entering:

```
logon shared-id by surrogate-id
```

where:

shared-id
: is the shared user ID you want to access

surrogate-id
: is the user ID of the surrogate user who is trying to log on

For example, user PEGGYK, with a password of BOND7, can log on to the shared user ID TESTCASE as follows:

1. Enter:

   ```
   logon testcase by peggyk
   ```

2. RACF displays the password prompt:

   ```
   Enter your password,
   or
   To change your password, enter: ccc/nnn/nnn
        where ccc = current password, and nnn = new password
   ```

   She would enter:

   ```
   bond7
   ```

   If PEGGYK wants to change her password from BOND7 to E8JAN35, she enters:

   ```
   bond7/e8jan35/e8jan35
   ```

In this example, TESTCASE is the shared user ID and PEGGYK is the surrogate user. PEGGYK's password was changed, but TESTCASE's password remains the same.

Note: When you log on to your user ID, you may be accustomed to seeing the message:

```
ICH70002I YOUR PASSWORD WILL EXPIRE IN nn DAYS.
```

However, this message is not issued for a shared logon.

Entering a RACF Command Session

If you are entering a RACF command session while logged on to a shared user ID and RACF prompts you for a password, enter your own password or password phrase. You do not need to know the shared user ID's password.

Special Considerations

General users need to consider the following when using the LOGON BY function.

Password Considerations

RACF verifies the password of the surrogate user, not that of the shared user ID. Therefore, the surrogate user's ID is revoked if the maximum number of incorrect passwords is exceeded while attempting to logon to the shared user ID.

If the surrogate user's CP directory password were NOPASS, RACF does not require a password when logging on to any shared user ID from that user ID.

Ownership Considerations

If your user ID is defined as shared, you may be able to permit other people to log on to your user ID as shared if you:

- Are the owner of the SURROGAT profile

  or

- Have ALTER access to the SURROGAT profile

If either if these conditions is true, you should be aware that when a surrogate user logs on to your user ID, the surrogate user has the authority to permit other users to log on or prevent other users from logging on to your user ID.

Terminal Considerations

If the TERMINAL class is active when a surrogate user attempts to logon to a shared user ID, both the shared user ID and the surrogate user must have access to the terminal being used.

Security Label Considerations

If the SECLABEL class is active, both the shared user and the surrogate user must be permitted to the appropriate SECLABEL profile. See *z/VM: RACF Security Server Security Administrator's Guide* for more information.

Changing How You Are Defined to RACF

You can change some of the ways RACF has defined you on the system by doing any or all of the following tasks:

- "Changing Your Password" on page 26
- "Changing your Password Phrase" on page 28
- "Changing Your Default Group" on page 30

- "Logging on with a Security Label" on page 23.
- "Logging On To Shared User IDs" on page 24.

Changing Your Password

Your user ID identifies you to RACF and your password verifies your identity. You have to change your password after a certain interval of time to help make sure that you are the only person who knows it. You can also make the time interval between changing your password shorter at the time you change your password.

For example, you should change your password if you suspect that your password has become known to others. Or, perhaps you would prefer to change your password more frequently than your installation requires.

Note: You may also change your password while logging on to the system. This is the most common way of changing your password. If your password has expired, RACF prompts you for a new password when you enter the old one. Before your password expires, you can clear the display, then enter the LOGON command with your user ID. RACF then prompts you for your password. At this time, you can enter both the current password and a new one.

RACF has the following rules for passwords:

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

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

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

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

Using the PASSWORD Command

To change your password, enter the PASSWORD command with the PASSWORD operand:

```
rac password password(current-password new-password)
```

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

```
rac password password(subject testers)
```

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

Changing Your Password Interval

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

```
rac password interval(interval-you-want)
```

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

```
rac password interval(15)
```

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

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

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

```
rac password password(current-password new-password) interval(nnn)
```

For example, to change your password from order to chaos and the interval to 99 days, type:

```
rac password password(order chaos) interval(99)
```

If you don't know your current password interval, enter the LISTUSER command and check the PASS-INTERVAL field. For more information, see “Finding Out How You Are Defined to RACF” on page 14.

Entering and Changing Your Password While Logging On

When logging on to z/VM, you can enter your user ID and password on the z/VM LOGON panel, and then hit the enter key. In this case, you will not see a password prompt (unless your password is expired, see below).

Alternatively, you can enter your password on the RACF password prompt. To get the password prompt, specify only your user ID on the z/VM LOGON panel, and then hit the enter key. Or, you can clear the display, then enter the LOGON command with only your user ID. In either case, RACF will display a password prompt. For example:

```
LOGON BRWELLS

Enter your password,
or
To change your password, enter: ccc/nnn/nnn
     where ccc = current password, and nnn = new password
```

This prompt gives you the option of changing your password before it has expired. Your passwords will not be visible on the display as you type them.

If you are logging on (by any of the methods described above) after your password has expired, RACF will prompt you to change it:

```
RPIMGR042I PASSWORD EXPIRED

To change your password - enter: nnn/nnn  where nnn = new password
or,
enter LOGOFF to cancel
```

You will not be able to LOGON to z/VM until you change your password. RACF will issue a message to confirm that your password has been changed:

```
HCPRPW004I Password changed
```

Note:

1. Depending on the options in effect on your system, you may get a warning message from RACF as your password approaches its expiration date. However, you will not actually be forced to change your password until it has actually expired.
2. You cannot specify a current password and a new password phrase, nor can you specify a current password phrase and a new password.

Changing your Password Phrase

Attention: Although RACF allows you to set and change a password phrase, other components may not support the use of a password phrase. Your installation might have applications that only support passwords.

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

RACF has the following rules for password phrases:

- The length can be 14 to 100 characters.

  Note: Your installation can choose to allow password phrases as short as 9 characters. Check with your security administrator or system programmer to find out if the lower limit has been implemented.
- The user ID (as sequential upper case characters or sequential lower case characters) can not be part of the password phrase
- At least 2 alphabetic characters must be specified (A - Z, a - z)
- At least 2 non-alphabetic characters must be specified (numerics, punctuation, special characters)
- Valid characters are:
  - Alphabetic uppercase (A–Z) and lowercase (a-z)
  - Numeric (0–9)
  - National (# (X'7B'), @ (X'7C'), and $ (X'5B'))
  - Punctuation
  - Special, except for the forward slash
  - Blank, but not leading or trailing blanks
- No more than 2 consecutive characters can be identical.

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

Using the PASSWORD or PHRASE Command

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

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

or

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

The current and new password phrases must have different values. Note that the password phrases must be entered in quotes. If the phrase value itself contains single quotation marks, they must be doubled. Take care to ensure that nobody can view your password phrase.

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

```
rac password phrase ('December 27, 1950' 'In 1492 Columbus sailed the ocean blue')
```

or

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

The password interval (that is, the time allowed before you are required to change your password again) also applies to the password phrase. For a description of how to change the password interval, see “Using the PASSWORD Command” on page 26. You can use either the PASSWORD or PHRASE command. For example, to change your password interval to 15 days, enter either of the following commands:

```
rac password interval(15)
```

or

```
rac phrase interval(15)
```

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

Entering and Changing Your Password Phrase While Logging On

The information in the section titled “Entering and Changing Your Password While Logging On” on page 27 is true for password phrases as well. Keep in mind the following considerations for password phrases:

- Do not enclose your password phrase in single quotation marks at the password prompt and don't double any single quotation marks which are actually part of your password phrase value.
- The prompt you receive, and subsequent error and warning messages, will contain the string "password", but they apply equally to password phrases. For example, if you specify a password phrase when logging on, and you receive a RACF message warning you that your password will soon expire, you can assume that the message refers to your password phrase.
- When entering a password phrase on the LOGON panel or in the LOGON command image, it is under the control of z/VM, and not RACF. Different rules may apply when using LOGON, as opposed to entering the phrase at the RACF password prompt. See *z/VM: CP Commands and Utilities Reference* for more information on the CP LOGON command.

Changing Your Default Group

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

To change your default group:

Notes:

- Use this procedure *only if* your installation does not have list-of-groups processing in effect. Ask your security administrator.
- If you belong to more than one group, and have no trouble accessing information belonging to the various groups, you need not use this procedure.

1. Determine what groups you belong to.

   You must first belong to a group before you can make it your default group. If you know that you belong to the group you need, proceed with Step 2.

   If you do not know whether you belong to the group you need, use the LISTUSER command, as described in "Finding Out How You Are Defined to RACF" on page 14, to see a list of the groups to which you belong.
2. Determine if you have the authority to make a group your default group.

   To make a group your default group you must be already connected to the group with at least USE authority. If you know you have the authority you need, proceed with Step 3.

   If you do not know whether you have the necessary authority, use the LISTUSER command, as described in "Finding Out How You Are Defined to RACF" on page 14. Look at the AUTH field in the portion of the RACF information that describes the group you belong to. The field must specify that you have at least USE authority.
3. Change your default connect group.

   Enter:

   ```
   rac altuser dfltgrp(group-name)
   ```

   The group name is the name of the group you want to make your default group when you log on.

   For example, to change your default group to devo, enter:

   ```
   rac altuser dfltgrp(devo)
   ```
4. Log off and log on again.

   The next time you log on, the new group you have made your default group is your current connect group. You still remain connected to your old group.

Chapter 5. Protecting Minidisks

Your RACF security administrator uses RACF to protect your minidisk. The security administrator creates a minidisk profile to protect a minidisk. *Minidisk profiles* contain a description of a minidisk, including the authorized users and the access authority of each user. A profile can either be discrete or generic. *Discrete profiles* protect only one minidisk. *Generic profiles* can protect zero or more minidisks at one time.

You can find out how your security administrator has done this by reading the following sections:

- "Finding Out About Your Minidisk Profiles"
- "Finding Out How a Minidisk Is Protected" on page 32.

Finding Out About Your Minidisk Profiles

You can have RACF list the names of the profiles you own. To list your minidisk profiles:

- Determine whether or not you belong to an ACIGROUP by entering:

  ```
  RACGROUP
  ```

  Note: RACGROUP is an EXEC and therefore can be entered directly. The RAC command or a RACF command session are not required.

  If you belong to an ACIGROUP, the group name is returned to you. Otherwise, a message is returned to you that the ACIGROUP for your user ID does not exist.

- If you belong to an ACIGROUP, determine what minidisk profiles you have by issuing the SEARCH command with the CLASS(VMMDISK) and MASK operands as follows:

  ```
  RAC  SEARCH CLASS(VMMDISK) MASK(your-acigroup.your-userid.)
  ```

  For example, if your user ID is ADAMS and your ACIGROUP is GROUP1, type:

  ```
  RAC  SEARCH CLASS(VMMDISK) MASK(GROUP1.ADAMS.)
  ```

  RACF lists all your minidisk profiles. For example, if two minidisks are protected with discrete profiles, you might see:

  ```
  GROUP1.ADAMS.191
  GROUP1.ADAMS.193
  ```

- If you do not belong to an ACIGROUP, determine what minidisk profiles you have by issuing the SEARCH command with the CLASS(VMMDISK) and MASK operands as follows:

  ```
  RAC  SEARCH CLASS(VMMDISK) MASK(your-userid.)
  ```

  For example, if your user ID is ADAMS, type:

  ```
  RAC  SEARCH CLASS(VMMDISK) MASK(ADAMS.)
  ```

  RACF lists all your minidisk profiles. For example, if two minidisks are protected with discrete profiles, you might see:

  ```
  ADAMS.191
  ADAMS.193
  ```

If you do not have any minidisk profiles, RACF displays a message stating that no entries meet the search criteria. Check that you have spelled everything correctly on the SEARCH command. If you have, inform your RACF security administrator that you have a minidisk which is not protected by RACF. Ask that a RACF profile be created for it.

Finding Out How a Minidisk Is Protected

If you are the owner of a minidisk (or you are responsible for the security protection of a minidisk), you may want to determine what protection the minidisk has. For example, you might want to find out what users and groups can access the minidisk.

Information You Need To Know First

You need to know the virtual address of the minidisk. If you have a minidisk accessed as A, the virtual address is, by convention, 191. To find the virtual address of one of your minidisks, enter the following CMS command:

QUERY DISK *n*

where *n* is the letter by which you know the minidisk. For example, for the address of your A-disk, enter:

```
QUERY DISK A
```

The virtual address of the minidisk is under the column labeled CUU or the column labeled VDEV on your screen.

Which Procedure to Use

You can choose between two procedures:

- If you are working with your own minidisk (such as your A-disk), try using the RACFLIST EXEC. This is described in “Procedure Using the RACFLIST EXEC” on page 33. Using RACFLIST does not require ISPF to be installed on your system.
- If you are working with a minidisk that you do not own (such as another user's minidisk), use the RACF commands described in “Procedure Using RACF Commands” on page 34.

Procedure Using the RACFLIST EXEC

Note: RACFLIST is an EXEC and therefore can be entered directly. You do not have to explicitly enter an appropriate RAC command; this is done by the RACFLIST EXEC. If you have problems using the RACFLIST EXEC, see your security administrator.

Enter:

```
racflist
```

and RACF displays the following panel:

```
----------------------  LIST ACCESS TO DISKS OR READER  ---------------------


 Enter the required data and press ENTER and then press PF2:


 AUTHORIZED USERS   ===>            Enter an S for a list of authorized users
 STATISTICS         ===>            ENTER AN S FOR A STATISTICS REPORT
 HISTORY            ===>            Enter an S for a HISTORY report

 READER             ===>            Enter an S for a report for the READER
 DISKS:             ===>            Enter the disk addresses for which you
                    ===>            want a report
                    ===>
                    ===>
                    ===>
                    ===>
                    ===>
                    ===>

1=Help  2=Execute 3=Quit  4=Clear 10=Authuser 11=Cmd line 12=Resources
Enter CP/CMS Commands below:
====>
```

Note: Press PF1 twice for online help.

On the panel, type in the following:

- For the AUTHORIZED USERS field, specify S if you want to display the access list of the minidisk profile.
- For the STATISTICS field, specify S if you want to display the number of times the minidisk was accessed by users.
- For the HISTORY field, specify S if you want to display information such as the date the minidisk profile was defined to RACF and the date on which the profile was last checked for UPDATE authority.
- Leave the READER field blank.
- For the DISKS fields, specify the virtual address of each minidisk for which you want information. (If you don't know the virtual address of the minidisk, see “Information You Need To Know First” on page 32.)

Press ENTER and PF2 to request that the information be listed. RACF displays a listing similar to that shown in Figure 7 on page 35. After the information is displayed, press PF4 to clear your terminal screen, then press PF3 to leave RACFLIST.

Note: The output of the RACFLIST EXEC is saved in the RACF DATA file until another RACF command is entered.

Procedure Using RACF Commands

Determine if a RACF profile protects the minidisk by issuing the RLIST command as follows:

```
RAC  RLIST  VMMDISK  userid.virtual-address  ALL
```

(If you don't know the virtual address of the minidisk, see "Information You Need To Know First" on page 32.)

For example, to determine if a RACF profile protects JBROWN's A-disk, use the following command:

```
RAC  RLIST  VMMDISK  JBROWN.191  ALL
```

You see one of the following on your screen:

- A listing for that profile, if the minidisk is protected by a discrete profile.
- A listing for the most specific generic profile that protects the minidisk, if the minidisk is not protected by a discrete profile but is protected by a generic profile, and generic profile command processing is active. (A generic profile is identified by a "G" in parentheses following the profile name.)
- A message stating that no profile was found, if the minidisk is not protected by a discrete or generic profile.

When a profile exists, you see a listing of the profile similar to that shown in Figure 7 on page 35.

When no profile exists, ask your RACF security administrator to create a profile to protect the minidisk.

```
CLASS         NAME
------        -----
VMMDISK       JBROWN.191

LEVEL    OWNER        UNIVERSAL ACCESS     YOUR ACCESS     WARNING
-----    -----        ----------------     -----------    -------
 00      JBROWN           READ               ALTER           NO

INSTALLATION DATA
-----------------
NONE

APPLICATION DATA
----------------
REVERIFY

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)
-------------     -------------------     --------------
 070    85          070        90            070     90

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

USER          ACCESS                ACCESS COUNT
----          ------                ------------
JBROWN        ALTER                    00009
```

Figure 7. Output of the RLIST Command for a Minidisk Profile

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

- LEVEL field (if used at your installation)
- OWNER field
- UNIVERSAL ACCESS field
- WARNING field
- SECLEVEL field (if used at your installation)
- CATEGORIES field (if used at your installation)
- SECLABEL field (if used at your installation)
- USER field and its related ACCESS and ACCESS COUNT fields.

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

CLASS
The name of the class to which the resource belongs.

NAME
The name of the discrete or generic profile.

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

OWNER
Each RACF-defined minidisk has an owner. An owner may be a user or a group. When you RACF-protect a minidisk without specifying an owner, RACF names you the owner of the minidisk profile. The owner of the profile may modify the minidisk profile.

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

YOUR ACCESS
How you may access this minidisk.

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

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

If this field contains NO, RACF does not permit a user with insufficient authority to access this resource.

Access or denial to the resource is determined by your installation.

INSTALLATION DATA
Any information your installation keeps in this minidisk profile.

APPLICATION DATA
Any information that RACF associates with the named resource.

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

CATEGORIES
Your installation can define its own security categories. These names are the security categories you need to access a resource protected by this profile.

SECLABEL
Your installation can define its own security labels. This security label is a

name used to represent the association between a particular security level and a set of zero or more categories. The security label displayed is the minimum security label you need to access a resource protected by this profile.

AUDITING
The type of access attempts that are recorded. In this example, the AUDITING is NONE. RACF does not record any attempts to update the minidisk.

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

CREATION DATE
The date the profile was created.

LAST REFERENCE DATE
The last time the profile was accessed.

LAST CHANGE DATE
The last time the profile was changed.

ALTER COUNT
The total number of times the minidisk protected by the profile was altered (not present for generic profiles).

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

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

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

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

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

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

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

USER, ACCESS, and ACCESS COUNT
Any specific users or groups permitted access to the minidisk. These fields describe the access list. USER is the user ID or group ID given the access authority listed in the ACCESS field. ACCESS COUNT is the number of times the user listed in the USER field accessed the minidisk (not present for generic profiles).

Note:

1. If your RACF security administrator has chosen not to record statistics for the VMMDISK class, these values do not change.

2. The z/VM control program does not call RACF when a user is linking to his or her own minidisk. Thus, RACF cannot maintain an access count for the minidisk owner's accesses.

Changing Access to a Minidisk

Situations may occur where you want to allow or deny someone the use of a minidisk that you have already protected. You may also change how users not included on the minidisk's access list may use the minidisk.

You can change the access to a minidisk by using the methods described in the following sections:

- "Changing the Universal Access Authority to a Minidisk"
- "Permitting an Individual or a Group to Use a Minidisk" on page 39
- "Denying an Individual or a Group Use of a Minidisk" on page 41.

Changing the Universal Access Authority to a Minidisk

You can allow other users to access a minidisk by specifying a universal access authority (UACC). This access authority would pertain to any user on the system. For example, you may have a minidisk containing research data which you need to protect so that no one can tamper with the data. You may want to change the universal access authority of the minidisk.

To change the universal access authority for a minidisk:

1. Find the name of the profile that protects the minidisk. To do this, see "Finding Out How a Minidisk Is Protected" on page 32.

   Remember that changing the UACC for a generic profile changes the access to all minidisks protected by the profile.
2. Decide which level of UACC to specify in the profile.

   The UACC can be one of the following: NONE, READ, UPDATE, CONTROL, or ALTER. For descriptions of these values, see "Access Authority for Minidisks on z/VM" on page 71.

Attention

- Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected minidisk can create copies of the data files on it. If a user copies the data files to a minidisk for which he/she can control the security characteristics, the user can downgrade the security characteristics of the copied files. For this reason, you may want to initially assign a UACC of NONE, and then selectively permit a small number of users to access your minidisk, as their needs become known. (For information on how to permit selected users or groups to access a minidisk, see "Permitting an Individual or a Group to Use a Minidisk" on page 39.)
- If you are changing the UACC to restrict access, be certain that any user or group specifically mentioned in the access list has the access to the resource that you intend. For example, if you change the UACC to NONE, and there is a user specifically named in the access list with any authority, that user still has that authority to the resource.

3. Change the UACC specified in the profile.

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

   ```
   RAC  RALTER  VMMDISK  profile-name  UACC(access-authority)
   ```

   Example 1:

   To change the UACC for minidisk ASMITH.191 to NONE, enter the following command:

```
RAC  RALTER  VMMDISK  ASMITH.191  UACC(NONE)
```

Example 2:

To change the UACC for the generic profile ASMITH.* to NONE, enter the following command:

```
RAC  RALTER  VMMDISK  ASMITH.*  UACC(NONE)
```

Permitting an Individual or a Group to Use a Minidisk

Besides protecting a minidisk with a universal access authority, you can give certain users different access authorities to use your minidisks. You add their user ID and the authority you want to give them to the access list on the minidisk profile. For example, if you would like J.E. Jones, whose user ID is JONES, to use your RACF-protected minidisk, you would add his user ID to its access list.

To permit an individual or a group use of a minidisk:

Note: For a description of when a change to a user's access occurs, see Appendix D, “When Minidisk Profile Changes Take Effect,” on page 75.

Choosing a Procedure

You can choose between two procedures:

- If you are working with your own minidisk (such as your A-disk), try using the RACFPERM EXEC. This is described in “Using the RACFPERM EXEC.” The RACFPERM EXEC displays a panel, but does not require ISPF to be installed on your system.
- If you are working with a minidisk that you do not own (such as a group minidisk or another user's minidisk), use the RACF commands described in “Using RACF Commands” on page 40.

Using the RACFPERM EXEC:

Note: RACFPERM is an EXEC and therefore can be entered directly. You do not have to explicitly enter an appropriate RAC command; this is done by the RACFPERM EXEC. If you have problems using the RACFPERM EXEC, see your security administrator.

Enter:

```
racfperm
```

and RACF displays the following panel:

```
 ----------------------  PERMIT ACCESS TO DISKS OR READER  --------------------

  Enter the required data and press ENTER and then press PF2:

  RESOURCE          ===>           DISK ADDRESS (191, 192, ETC.) OR RDR
  ACCESS AUTHORITY  ===>           DELETE  - TO REMOVE ACCESS AUTHORITY
                                   NONE    - TO PREVENT A USER FROM ACCESSING
                                   READ    - TO ALLOW READ/ONLY ACCESS
                                   UPDATE  - TO ALLOW WRITE ACCESS
                                   CONTROL - TO ALLOW MULTI-READ ACCESS
                                   ALTER   - TO ALLOW MULTI-WRITE ACCESS  (also
                                             allows user to assign authority)
  Enter the userids and/or groupids whose access authority you want to change:

  USERIDS AND/OR GROUPIDS:
  ===>             ===>             ===>             ===>
  ===>             ===>             ===>             ===>
  ===>             ===>             ===>             ===>
  ===>             ===>             ===>             ===>

1=Help  2=Execute 3=Quit  4=Clear 10=Authority 11=Cmd line 12=User IDs
Enter CP/CMS Commands below:
====>
```

Note: Press PF1 twice for online help.

On the panel, type in the following:

- For the RESOURCE field, specify the virtual address of the minidisk you want to grant access to. For example, for your A-disk, specify 191.
- For the ACCESS AUTHORITY field, specify the access authority you want to grant.
- In the USERIDS AND/OR GROUPIDS fields, specify the user IDs or group IDs (group names) to which you want to grant access.

Press ENTER and PF2 to execute the request.

After RACF displays some messages related to the request, press PF4 to clear your terminal screen, then press PF3 to leave RACFPERM.

Note: The output of the RACFPERM EXEC is saved in the RACF DATA file until another RACF command is entered.

Using RACF Commands:

1. Find the name of the profile that protects the minidisk. To do this, see "Finding Out How a Minidisk Is Protected" on page 32.
2. Decide which access authority to specify in the profile.

   The access authority can be one of the following: NONE, READ, UPDATE, CONTROL, and ALTER. For descriptions of these values, see "Access Authority for Minidisks on z/VM" on page 71.

Attention

Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected minidisk can create copies of the data files on it. If a user copies the data files to a minidisk for which he/she can control the security characteristics, the user can downgrade the security characteristics of the copied files. For this reason, you may want to initially assign a UACC of NONE, and then selectively permit a small number of users to access your minidisk, as their needs become known.

3. Allow access to a minidisk.

To allow access to your minidisk, use the PERMIT command with the ACCESS operand. Type:

```
RAC  PERMIT  profile-name  CLASS(VMMDISK)  ID(user ID or group ID)
             ACCESS(level)
```

Example 1:

To permit user Jones to read the user minidisk DCOLLINS.191, type:

```
RAC  PERMIT DCOLLINS.191 CLASS(VMMDISK) ID(JONES) ACCESS(READ)
```

Example 2:

To permit users Jones and Moore to read the user minidisk DCOLLINS.191, type:

```
RAC  PERMIT DCOLLINS.191 CLASS(VMMDISK) ID(JONES, MOORE)  ACCESS(READ)
```

Example 3:

To permit group DEPTD60 to read the user minidisk DCOLLINS.191, type:

```
RAC  PERMIT DCOLLINS.191 CLASS(VMMDISK) ID(DEPTD60) ACCESS(READ)
```

Example 4:

To permit groups DEPTD60 and DEPTD58 to read the user minidisk DCOLLINS.191, type:

```
RAC  PERMIT DCOLLINS.191 CLASS(VMMDISK) ID(DEPTD60, DEPTD58)
            ACCESS(READ)
```

Denying an Individual or a Group Use of a Minidisk

As described in "Finding Out How a Minidisk Is Protected" on page 32, you can use a minidisk profile to protect the information you create and use to do your job. You may want to deny an individual use of a minidisk. For example, a colleague who has left the department can still use a minidisk. For security reasons you would wish to exclude the person from using the minidisk. You can deny anyone access to your minidisk by specifying a certain universal access or individual access authority.

Note: For a description of when a change to a user's access occurs, see Appendix D, "When Minidisk Profile Changes Take Effect," on page 75.

To deny an individual or a group use of a minidisk:

Choosing a Procedure

You can choose between two procedures:

- If you are working with your own minidisk (such as your A-disk), try using the RACFPERM EXEC. This is described in "Using the RACFPERM EXEC." Using RACFPERM does not require ISPF to be installed on your system.
- If you are working with a minidisk that you do not own (such as a group minidisk or another user's minidisk), use the RACF commands described in "Using RACF Commands" on page 42.

Using the RACFPERM EXEC:

Note: RACFPERM is an EXEC and therefore can be entered directly. You do not have to explicitly enter an appropriate RAC command; this is done by the RAC EXEC. The RAC command or a RACF command session are not required.

Enter:

```
racfperm
```

and RACF displays the following panel:

```
----------------------  PERMIT ACCESS TO DISKS OR READER  --------------------

 Enter the required data and press ENTER and then press PF2:

 RESOURCE          ===>          Enter your current password
 ACCESS AUTHORITY  ===>          DISK ADDRESS (191, 192, ETC.) OR RDR
                                 DELETE  - TO REMOVE ACCESS AUTHORITY
                                 NONE    - TO PREVENT A USER FROM ACCESSING
                                 READ    - TO ALLOW READ/ONLY ACCESS
                                 UPDATE  - TO ALLOW WRITE ACCESS
                                 CONTROL - TO ALLOW MULTI-READ ACCESS
                                 ALTER   - TO ALLOW MULTI-WRITE ACCESS  (also
                                           allows user to assign authority)
 Enter the userids and/or groupids whose access authority you want to change:

 USERIDS AND/OR GROUPIDS:
 ===>             ===>             ===>             ===>
 ===>             ===>             ===>             ===>
 ===>             ===>             ===>             ===>
 ===>             ===>             ===>             ===>

1=Help  2=Execute 3=Quit  4=Clear 10=Authority 11=Cmd line 12=User IDs
Enter CP/CMS Commands below:
====>
```

Note: Press PF1 twice for online help.

On the panel, type in the following:

- For the RESOURCE field, specify the virtual address of the minidisk you want to deny access to. For example, for your A-disk, specify 191.
- For the ACCESS AUTHORITY field, specify DELETE or NONE.

  Note: DELETE removes the name of the user or group from the access list. However, this denies access only if the UACC is NONE. For example, if you delete a user or group from the access list but the UACC is READ or higher, the user or group still has access to the minidisk. To ensure that the user or group cannot access the minidisk, specify NONE.
- In the USERIDS AND/OR GROUPIDS fields, or both, specify the user IDs or group IDs (group names) whom you want to deny access.

Press ENTER and PF2 to execute the request.

After RACF displays some messages related to the request, press PF4 to clear your terminal screen, then press PF3 to leave RACFPERM.

Note: The output of the RACFPERM EXEC is saved in the RACF DATA file until another RACF command is entered.

Using RACF Commands:

1. Find the name of the profile that protects the minidisk. To do this, see "Finding Out How a Minidisk Is Protected" on page 32.
2. Deny access to a minidisk.

   You can deny access to a minidisk in two ways.

   - One way is to remove the name of the user or group from the access list. However, this denies access only if the UACC is NONE. For example, if you delete a user or group from the access list but the UACC is READ or higher,

the user or group still has access to the minidisk. See "Removing the Individual or Group From the Access List."

- The second way to deny access is to include the user or group on the access list but assign the user or group an access of NONE. Assigning an access of NONE is the best way to make sure the user or group cannot access the minidisk. See "Assigning the User or Group an Access of NONE."

Assigning the User or Group an Access of NONE

Including the user or group on the access list with ACCESS(NONE) is the best way to ensure that the user or group cannot access the minidisk.

To deny access by assigning a user or group an access of NONE, enter the PERMIT command with the ACCESS keyword as follows:

```
RAC  PERMIT profile-name  CLASS(VMMDISK) ID(user ID or group ID)  ACCESS(NONE)
```

Example 1:

To deny user Jones use of user minidisk KIRBY.191, type:

```
RAC  PERMIT  KIRBY.191  CLASS(VMMDISK) ID(JONES) ACCESS(NONE)
```

Example 2:

To deny users Jones and Moore the use of user minidisk KIRBY.191, type:

```
RAC  PERMIT KIRBY.191 CLASS(VMMDISK) ID(JONES, MOORE) ACCESS(NONE)
```

Example 3:

To deny group DEPTD60 use of user minidisk KIRBY.191, type:

```
RAC  PERMIT  KIRBY.191  CLASS(VMMDISK)  ID(DEPTD60)  ACCESS(NONE)
```

Example 4:

To deny groups DEPTD60 and DEPTD58 use of user minidisk KIRBY.191, type:

```
RAC  PERMIT KIRBY.191 CLASS(VMMDISK) ID(DEPTD60, DEPTD58) ACCESS(NONE)
```

Removing the Individual or Group From the Access List

To deny access by removing a user or a group from the access list, enter the PERMIT command with the DELETE operand:

```
RAC  PERMIT  profile-name  CLASS(VMMDISK)  ID(user ID or group ID) DELETE
```

Example 1:

To deny user Jones use of user minidisk DLEWIS.191, enter:

```
RAC  PERMIT  DLEWIS.191  CLASS(VMMDISK)  ID(JONES)  DELETE
```

Example 2:

To deny users Jones and Moore use of user minidisk DLEWIS.191, type:

```
RAC  PERMIT DLEWIS.191 CLASS(VMMDISK)  ID(JONES, MOORE) DELETE
```

Example 3:

To deny group DEPTD60 use of user minidisk DLEWIS.191, type:

```
RAC  PERMIT  DLEWIS.191  CLASS(VMMDISK)  ID(DEPTD60)  DELETE
```

Example 4:

To deny groups DEPTD60 and DEPTD58 use of user minidisk DLEWIS.191, type:

```
RAC  PERMIT  DLEWIS.191  CLASS(VMMDISK)  ID(DEPTD60, DEPTD58)  DELETE
```

Chapter 6. Protecting SFS Files and Directories

The *shared file system* (*SFS*) is a facility for organizing user files on z/VM. Related files can be grouped together into directories. RACF provides access authorization for SFS files and directories through the use of profiles. Using RACF commands, you can:

- Add, delete, change, list, and search for profiles
- Change access lists.

Notes:

- These tasks are only valid if your installation is using RACF to protect SFS files and directories. Check with your security administrator.
- For information about RACF profiles, see Chapter 5, "Protecting Minidisks," on page 31.

Working with SFS Files

Get a List of SFS File Profiles

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.

SRFILE Examples

1. To list all of your file profiles, enter:

   ```
   rac srfile filter(* * pool1:laurie.**)
   ```

2. To list all file profiles you have at least READ access to, enter:

   ```
   rac srfile
   ```

Add a Profile for an SFS File

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

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.**
```

ADDFILE Examples

1. LAURIE is your user ID. To protect a file called PROGRAM NOTES in your SHOW directory and notify BRUCE if RACF denies access to the file, create a discrete profile:

   ```
   rac addfile program notes pool1:laurie.show notify(bruce)
   ```

   The default values are:

   owner(laurie)

   audit(failures(read))

   level(0)

List Information in an SFS File Profile

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.

The details RACF lists from each file profile are:

- The level
- The owner
- 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
- Installation-defined data as specified on the DATA operand of the ADDFILE or ALTFILE command
- Application-defined data as specified on the APPLDATA operand of the ADDFILE or ALTFILE command
- The status of the WARNING | NOWARNING indicator

You can request additional details as follows:

- Historical data, such as:
  - Date the file was defined to RACF
  - Date the file was last referenced
  - Date the file was last updated.
- The number of times the file was accessed by all users for each of the following access authorities:

  ALTER, CONTROL, UPDATE, READ.
- A list of:
  - 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

Specify LFILE with the AUTHUSER operand 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
- 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.

LFILE Examples

1. Suppose your user ID GENE is defined to RACF and you do not have the AUDITOR attribute. To list the information for the profile protecting the file CHART NOTES in your TOP40 subdirectory, enter:

```
rac lfile chart notes livrpool:gene.top40 all
```

Figure 8 shows the output from this command.

```
LFILE CHART NOTES LIVRPOOL:GENE.TOP40 ALL

     CLASS       NAME
     -----       ----
     FILE        CHART NOTES LIVRPOOL:GENE.TOP40

     LEVEL  OWNER    UNIVERSAL ACCESS  YOUR ACCESS   WARNING
     -----  -------- ----------------  -----------   -------
      00    GENE           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)
     -------------  -------------------  ----------------
       303    95          333    95         333    95

     ALTER COUNT   CONTROL COUNT   UPDATE COUNT   READ COUNT
     -----------   -------------   ------------   ----------
       000000         000000         000000         000000

     USER      ACCESS   ACCESS COUNT
     ----      ------   ------ -----
     GENE      ALTER       000000

     NO ENTRIES IN CONDITIONAL ACCESS LIST
```

Figure 8. LFILE Command Output

Change a Profile for an SFS File

Use the ALTFILE command to modify existing RACF profiles protecting SFS files. After you alter a generic profile, you or others affected by the change need to log off and then log back on so the changes will take effect.

ALTFILE Examples

1. To notify BRUCE whenever an unauthorized person tries to gain access to the PROGRAM NOTES file in your SHOW directory, enter:

   ```
   rac altfile program notes pool:laurie.show notify(bruce)
   ```

Maintain SFS File Access Lists

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.

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.

After you alter a generic profile, you need to log off and then log back on so the changes will take effect.

PERMFILE Examples

1. Suppose your user ID SUSAN and another user's ID, LIZ, are defined to RACF, and your file pool ID is POOL3. To authorize LIZ so she can update a file called QUILT PROJECTS in your FABRIC directory, enter:

   ```
   rac permfile quilt projects pool3:susan.fabric acc(update) id(liz)
   ```

Delete a Profile for an SFS File

Use the DELFILE command to delete a discrete or generic profile from the RACF database. The file itself is not physically deleted or “scratched.”

DELFILE Examples

1. To delete the discrete profile that protects your PROGRAM NOTES file, enter:

   ```
   rac delfile program notes pool1:laurie.
   ```

Working with SFS Directories

Get a List of SFS Directory Profiles

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.

SRDIR Examples

1. You are defined to RACF. To find out which SFS directory profiles you have at least READ access to, enter:

   ```
   rac srdir
   ```

2. The user ID PEGGY is defined to RACF and has a file pool ID of POOL2. To determine which directory profiles belong to PEGGY, enter:

   ```
   rac srdir filter(pool2:peggy.**)
   ```

Add a Profile for an SFS Directory

Use the ADDDIR command to RACF-protect an SFS directory with a discrete profile or a generic profile. A *discrete profile* is a resource profile that can provide RACF protection for only a single resource. For example, a discrete profile can protect only a single SFS directory. A *generic profile* is a resource profile that can provide RACF protection for one or more resources. For example, a discrete profile can protect one or more SFS directories.

The ADDDIR command adds a profile to the RACF database in order to control access to one or more SFS directories. It also places your user ID on the access list and gives you ALTER authority to the SFS directory.

ADDDIR Examples

1. Suppose your user ID LAURIE is RACF-defined and you own a directory called DIR1 in file pool POOL1. To protect your directory, create a discrete profile:

   ```
   rac adddir pool1:laurie.dir1 uacc(none)
   ```

   The default values are:

   owner(laurie)

   audit(failures(read))

   level(0)

2. Suppose your user ID LAURIE is also authorized to a security label called SECRET. To protect your directory (classified as SECRET) and all of its subdirectories, create a generic profile:

   ```
   rac adddir pool1:laurie.dir1.** seclabel(secret) uacc(none)
   ```

   The default values are:

   owner(laurie)

   audit(failures(read))

   level(0)

List Information in an SFS Directory Profile

Use the LDIRECT command to list information included in directory profiles. You can request details for a specific profile by specifying the full name of the profile. You can also use the LDIRECT command to find the name of a profile that protects a directory.

Profiles are listed in alphabetic order. Generic profiles are listed in the same order as they are searched for a resource match.

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
- Installation-defined data as specified on the DATA operand of the ADDDIR or ALTDIR command
- Application-defined data as specified on the APPLDATA operand of the ADDDIR or ALTDIR command
- The status of the WARNING | NOWARNING indicator

You can request the following additional details:

- Historical data, such as:
  - Date the directory was defined to RACF
  - Date the directory was last referenced
  - Date the directory was last updated.
- The number of times the directory was accessed by all users for each of the following access authorities:

  ALTER, CONTROL, UPDATE, READ.
- A list of:
  - 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

Specify LDIRECT with the AUTHUSER operand 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
- 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.

LDIRECT Examples

1. Suppose your user ID GENE is defined to RACF. To list all information for your BEATLES.ANTHOLOGY directory in file pool LIVRPOOL, enter:

   ```
   rac ldirect livrpool:gene.beatles.anthology all
   ```

   Figure 9 on page 53 shows the output from this command.

```
LDIRECT LIVRPOOL:GENE.BEATLES.ANTHOLOGY ALL

    CLASS       NAME
    -----       ----
    DIRECTRY    LIVRPOOL:GENE.BEATLES.ANTHOLOGY

    LEVEL  OWNER    UNIVERSAL ACCESS  YOUR ACCESS   WARNING
    -----  -------- ----------------  -----------   -------
     00    GENE           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)
    -------------  -------------------  ---------------
      324    95          342    95         342    95

    ALTER COUNT   CONTROL COUNT   UPDATE COUNT   READ COUNT
    -----------   -------------   ------------   ----------
      000000         000000         000000         000000

    USER      ACCESS   ACCESS COUNT
    ----      ------   ------ -----
    GENE      ALTER       000000

    NO ENTRIES IN CONDITIONAL ACCESS LIST
```

Figure 9. LDIRECT Command Output

Change a Profile for an SFS Directory

Use the ALTDIR command to modify an existing RACF profile protecting an SFS directory. After you alter a generic profile, you or others affected by the change need to log off and then log back on so the changes will take effect.

ALTDIR Examples

1. To make BRUCE the owner of LAURIE's SHOW directory, enter:

   ```
   rac altdir pool1:laurie.show owner(bruce)
   ```

2. To allow notification to come to your user ID LAURIE when an unauthorized user tries to access your DEPT directory, enter:

   ```
   rac altdir pool1:laurie.dept notify(laurie)
   ```

Maintain SFS Directory Access Lists

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.

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.

After you alter a generic profile, you or others affected by the change need to log off and then log back on so the changes will take effect.

PERMDIR Examples

1. Suppose your user ID EUGENE and another user's ID, JCARSON, are defined to RACF, and your file pool ID is POOL4. To authorize JCARSON to look at your HOUNDDOG directory, enter:

   ```
   rac permdir pool4:eugene.hounddog id(jcarson)
   ```

   The default values are:

   access(read)

Delete a Profile for an SFS Directory

Use the DELDIR command to delete a discrete or generic directory profile from the RACF database. The SFS directory itself is not physically deleted.

Note: If a physical directory that is protected by a discrete profile is deleted, the discrete profile is deleted as well.

DELDIR Examples

1. To delete the discrete profile for your PROJECT directory in the POOL1 file pool, enter:

   ```
   rac deldir pool1:laurie.project
   ```

Chapter 7. Protecting General Resources

The types of general resources that RACF can protect include:

- Minidisks
- Terminals
- Virtual unit record devices
- Alternate user IDs
- SFS files and directories
- SFS administrator and operator commands
- OpenExtensions resources
- Installation-defined resources.
- Guest LANs and virtual switches
- Some CP commands and DIAGNOSE instructions

Resources are protected with profiles. A profile contains descriptive information about a user, a group, or resource. RACF uses the information in a profile to control use of protected resources. When you attempt to use a protected resource, RACF checks your user profile, as well as the resource profile, to decide whether to allow you to use the resource.

Resource profiles describe the information and the levels of authority needed to use the resource. A resource profile contains:

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

  You can protect a resource by identifying specific users with the access you want them to have in the access list. All other users are allowed the access you specify as the universal access authority (UACC). The access authorities you can specify are: NONE, READ, UPDATE, CONTROL, and ALTER. See “Access Authority for General Resources” on page 73 for more information about access authorities. To protect a resource most effectively, you should initially specify a UACC of NONE and selectively give certain users specific access authority to the resource.

Note: The security administrator is *generally* the person who defines, alters, or deletes a general resource profile.

You can use RACF to protect your general resources by doing the tasks defined in the following sections:

- "Searching for General Resource Profile Names"
- "Listing the Contents of General Resource Profiles" on page 57
- "Permitting an Individual or a Group to Use a General Resource" on page 58
- "Denying an Individual or a Group Use of a General Resource" on page 58.

For more information about protecting:

- Minidisks, see Chapter 5, "Protecting Minidisks," on page 31
- SFS files and directories, see Chapter 6, "Protecting SFS Files and Directories," on page 45
- SFS administrator and operator commands, see *z/VM: RACF Security Server Security Administrator's Guide*
- OpenExtensions resources, see *z/VM: OpenExtensions User's Guide*

Searching for General Resource Profile Names

You can list the names of general resource profiles that you own by using the SEARCH command.

The SEARCH command searches the RACF database for the name of profiles (in a particular resource class) that match the criteria you specify. For example, you can search for all virtual unit record device profiles (which are found in the VMRDR class) that you are the owner of, or to which you have at least READ access.

The output of this command is in line mode unless you use ISPF panels. You can use the RACF DATA file that is generated when you use the RAC command processor.

Attention: Using the SEARCH command may slow the system's performance. Therefore, the SEARCH command should be used with discretion (or not at all) during busy system times.

1. Find the name of the class that represents the resource you want to search. Valid class names are DATASET, USER, GROUP, and those specified in the class descriptor table (CDT). For a list of general resource classes defined in the IBM-supplied CDT, see Appendix E, "Description of RACF Classes," on page 77.
2. Request the list of RACF profiles for the class. To search the RACF database for general resource profiles that you own, use the SEARCH command with the CLASS operand:

   ```
   rac search class(classname)
   ```

   To find all the general resources you can access, this must be done one class at a time.

Example:

To search for resource profiles in class VMRDR, enter:

```
rac search class(vmrdr)
```

Other Operands of the SEARCH Command

These examples show only some of the operands that are available to use on the SEARCH command. The complete syntax of the SEARCH command, with descriptions of all the command operands, is described in *z/VM: RACF Security Server Command Language Reference*. In particular, you may want to read about FILTER operand, which specifies a string of characters to be used in searching the RACF database. The filter string defines the range of profile names you want to select from the RACF database.

Listing the Contents of General Resource Profiles

You can list the contents of general resource profiles that you own by using the RLIST command.

The RLIST command lists the contents of general resource profiles in a particular resource class. If you specify a profile that you do not have access to, you may receive an "access violation" message from the RLIST command.

Note: To see the access list for a resource, you must be the owner of the resource, or have ALTER access to the resource.

1. Find the name of the class that represents the resource you want to search. Valid class names are 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 E, "Description of RACF Classes," on page 77.
2. Specify the RACF profiles you want to list. To list the contents of general resource profiles that you own, use the RLIST command with the class name and a profile name:

   rac rlist *classname profile-name*

Example 1:

To list the contents of resource profile LAURIEW in class VMRDR, enter:

```
rac rlist vmrdr lauriew
```

Example 2:

To list the contents of all resource profiles in class VMRDR that you are the owner of, or to which you have at least READ access, enter:

```
rac rlist vmrdr *
```

Other Operands of the RLIST Command

These examples show only some of the operands that are available to use on the RLIST command. The complete syntax of the RLIST command, with descriptions of all the command operands, is described in *z/VM: RACF Security Server Command Language Reference*. In particular, you may want to read about:

- ALL, which displays all information specified for each resource.
- AUTHUSER, which displays the standard and conditional access lists for the profile. This is useful information to have before you use the PERMIT command to allow or deny access to the resource.

Permitting an Individual or a Group to Use a General Resource

You can give certain users or groups of users different access authorities to use a general resource. You add their user ID and the authority you want to give them to the access list on the resource profile. For example, if you would like B.R. Wells, whose user ID is BRWELLS, to be able to send files to your RACF-protected virtual reader, you would add his user ID to its access list.

To permit an individual or a group to use a general resource:

1. Find the name of the profile that protects the general resource. To do this, see "Searching for General Resource Profile Names" on page 56.
2. Decide which access authority to specify in the profile. The access authority can be one of the following: NONE, READ, UPDATE, CONTROL, and ALTER. For descriptions of these values, see "Access Authority for General Resources" on page 73.
3. Allow access to the general resource. To allow access to your general resource, use the PERMIT command with the ACCESS operand, enter:

   ```
   rac permit profile-name class(class-name) id(userid|groupid)
       access(access-authority)
   ```

Example 1:

To permit BRWELLS to have access to a virtual unit record device protected by general resource profile LAURIEW, enter:

```
rac permit lauriew class(vmrdr) id(brwells) access(update)
```

Example 2:

To permit groups DEPT58 and DEPT59 to have access to a virtual unit record device protected by general resource profile LAURIEW, enter:

```
rac permit lauriew class(vmrdr) id(dept58, dept59) access(update)
```

Other Operands of the PERMIT Command

These examples show only some of the operands that are available to use on the PERMIT command. The complete syntax of the PERMIT command, with descriptions of all the command operands, is described in *z/VM: RACF Security Server Command Language Reference*.

Denying an Individual or a Group Use of a General Resource

You may want to deny an individual or group use of a general resource. For example, a colleague who has left the department can still use a general resource. For security reasons you would wish to exclude the person from using the general resource. You can deny a person access to your general resource by specifying a certain universal access or individual access authority.

To deny an individual or a group the use of a general resource:

1. Find the name of the profile that protects the general resource. To do this, see "Searching for General Resource Profile Names" on page 56.
2. Deny access to the general resource. You can deny access in one of two ways:
   - One way is to remove the name of the user or group from the access list. However, this denies access only if the UACC is NONE. For example, if you delete a user or group from the access list but the UACC is READ or higher,

the user or group still has access to the general resource. See "Removing the Individual or Group from the Access List."

- The second way to deny access is to include the user or group on the access list but assign the user or group an access of NONE. By assigning an access of NONE, you make sure the user or group cannot access the general resource. See "Assigning the User or Group an Access of NONE."

Assigning the User or Group an Access of NONE

By including the user or group on the access list with ACCESS(NONE), you make sure that the user or group cannot access the general resource.

To deny access by assigning a user or group an access of NONE, enter the PERMIT command with the ACCESS keyword as follows:

rac permit *profile-name* **class(***class-name***) id(***userid*|*groupid***) access(none)**

Example 1:

To deny user BRWELLS the ability to send files to a virtual reader protected by general resource profile LAURIEW, enter:

```
rac permit lauriew class(vmrdr) id(brwells) access(none)
```

Example 2:

To deny groups DEPT58 and DEPT59 the ability to send files to a virtual reader protected by general resource profile LAURIEW, enter:

```
rac permit lauriew class(vmrdr) id(dept58, dept59) access(none)
```

Other Operands of the PERMIT Command

These examples show only some of the operands that are available to use on the PERMIT command. The complete syntax of the PERMIT command, with descriptions of all the command operands, is described in *z/VM: RACF Security Server Command Language Reference*. In particular, you may want to read about RESET, which deletes the entire contents of both the standard access list and the conditional access list of a profile.

Removing the Individual or Group from the Access List

To revert to the universal access authority for a user or group, enter the PERMIT command with the DELETE operand, enter:

rac permit *profile-name* class(*class-name*) id(*userid*|*groupid*) delete

Example 1:

To remove user SUSANH from the access list for a terminal protected by general resource profile LAURIEW, enter:

```
rac permit lauriew class(vmrdr) id(susanh) delete
```

Access to the virtual reader for user SUSANH reverts to the universal access authority for the virtual reader.

Example 2:

To remove groups DEPT58 and DEPT59 from the access list for a terminal protected by general resource profile LAURIEW, enter:

```
rac permit lauriew class(vmrdr) id(dept58, dept59) delete
```

Access to the virtual reader for groups DEPT58 and DEPT59 reverts to the universal access authority for the virtual reader.

Other Operands of the PERMIT Command

These examples show only some of the operands that are available to use on the PERMIT command. The complete syntax of the PERMIT command, with descriptions of all the command operands, is described in *z/VM: RACF Security Server Command Language Reference*. In particular, you may want to read about RESET, which deletes the entire contents of both the standard access list and the conditional access list of a profile.

Appendix A. Profile Names for SFS Files and Directories

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 the command in the RACF command session on z/VM, you must specify the 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 6.

Table 6. 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.

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:
      1) 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.
      2) 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.
      3) 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:
      1) 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.
      2) 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 7 shows examples of these rules for specifying defaults in profile names for the FILE and DIRECTRY classes.

Table 7. 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 7. 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 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 8, Table 9, Table 10 on page 65, and Table 11 on page 65 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 8. 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 9. 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 10. 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 11. 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 "Generic Characters in SFS Names" on page 64.

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. Profile Names for General Resources

For naming general resources, you can use discrete or generic profiles. 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

The %* combination requires special attention. New profiles with an ending %* are not allowed, nor are profiles named %*. The RDEFINE command will return an error message. Existing profiles (created prior to RACF release 1.9) 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 12, Table 13, and Table 14 give examples of generic profile names for general resources.

Table 12. 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 13. 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 14. 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.

Table 15. 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

Appendix C. Access Authority for Resources

The access authority definitions that follow apply to universal access authority (UACC) and to authority granted to individual users or groups in the resource profile access list.

The UACC is the default **resource-access authority**. All users or groups of users in the system who are not specifically named in an access list of authorized users for that resource can still access the resource with the authority specified by the UACC.

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.

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*.

Access Authority for SFS Files and Directories

SFS files and directories on z/VM can have one of these access authorities:

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

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 he or she can control the security characteristics, the user 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 "Maintain SFS Directory Access Lists" on page 54for 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 file or directory for reading only.

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

CONTROL
Equivalent to UPDATE.

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

When ALTER is specified in a:

- Discrete profile, users can read, alter, and delete the profile itself, *including the access list*. However, ALTER does not allow users to change the owner of the profile.
- Generic profile, users have *no* authority over the profile itself.
- Generic DIRECTRY profile, users can create SFS directories protected by the profile.
- Generic FILE profile, users can 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 General Resources

Note: The access authorities that follow can have different meanings depending on the general resource they are protecting. See *z/VM: RACF Security Server Security Administrator's Guide* for information about the access authorities for each kind of general resource.

For general resources, access authority can be:

ALTER
Specifies that the user or group have full control over the resource.

CONTROL
Specifies that the user or group be authorized to access the resource for the purpose of reading or writing. This authority may have additional meaning depending on the general resource profile it is used for.

UPDATE
Specifies that the user or group be authorized to access the resource for the purpose of reading or writing.

READ
Specifies that the user or group be authorized to access the resource for the purpose of reading only.

NONE
Specifies that the user or group not be permitted to access the resource.

Appendix D. When Minidisk Profile Changes Take Effect

If a user is currently using your minidisk, changing the access of that user may not affect the current access until that user logs on again.

Your change affects the user's access immediately in the following cases:

- If the user is not logged on. You can check to see if a user is logged on with the CP QUERY command:

  `QUERY` *`userid`*

- If the user is logged on and has not yet linked to the minidisk. You can check to see if a user is linked to your minidisk with the CP QUERY LINKS command:

  `QUERY LINKS` *`virtual-address`*

If the user is logged on and has linked to the minidisk, and you change his access, two situations could occur:

- If the profile is a discrete profile, the user's access changes after detaching the minidisk.
- If the profile is a generic profile, the user's access changes after *both* the following occur:
  - The user detaches the minidisk.
  - The copy of the generic profile that is kept in virtual storage is changed.

  The copy of the generic profile is changed when the user logs off and on again or when the SETROPTS GENERIC REFRESH command is issued.

Appendix E. Description of RACF Classes

See *z/VM: RACF Security Server Macros and Interfaces* for more information on the IBM-supplied class descriptor table (CDT).

On z/VM systems, the following classes are defined in the IBM-supplied CDT:

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.
RVARSMBR	Member class for RACFVARS (not for use on RACF commands).
SCDMBR	Member class for SECDATA class (not for use on RACF commands).

Class	Purpose
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.
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.

On z/OS systems, the following classes are defined in the IBM-supplied CDT:

Table 16. z/OS classes

Class	Function
APPCLU	Verifying the identity of partner logical units during VTAM® session establishment.
APPCPORT	Controlling which user IDs can access the system from a given LU (APPC port of entry). Also, conditional access to resources for users entering the system from a given LU.
APPCSERV	Controlling whether a program being run by a user can act as a server for a specific APPC transaction program (TP).
APPCSI	Controlling access to APPC side information files.
APPCTP	Controlling the use of APPC transaction programs.
APPL	Controlling access to applications.
CBIND	Controlling the client's ability to bind to the server.
CONSOLE	Controlling access to MCS consoles. Also, conditional access to other resources for commands originating from an MCS console.
CSFKEYS	Controlling use of Integrated Cryptographic Service Facility/MVS (ICSF/MVS) cryptographic keys. See also the GCSFKEYS class.
CSFSERV	Controlling use of Integrated Cryptographics Service Facility/MVS (ICSF/MVS) cryptographic services.
DASDVOL	DASD volumes. See also the GDASDVOL class.

Table 16. z/OS classes (continued)

Class	Function
DEVICES	Used by z/OS allocation to control who can allocate devices such as: • Unit record devices (printers and punches) (allocated only by PSF, JES2, or JES3) • Graphics devices (allocated only by VTAM) • Teleprocessing (TP) or communications devices (allocated only by VTAM)
DIRAUTH	Setting logging options for RACROUTE REQUEST=DIRAUTH requests. Also, if the DIRAUTH class is active, security label authorization checking is done when a user receives a message sent through the TPUT macro or the TSO SEND, or LISTBC commands. Profiles are not allowed in this class.
DLFCLASS	The data lookaside facility.
DSNR	Controlling access to DB2® subsystems.
FACILITY	Miscellaneous uses. Profiles are defined in this class so that resource managers (typically program products or components) can check a user's access to the profiles when the users take some action. Examples are catalog operations (DFP) and use of the vector facility. 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 the product's documentation.
FIELD	Fields in RACF profiles (field-level access checking).
GCSFKEYS	Resource group class for CSFKEYS class. [1]
GDASDVOL	Resource group class for DASDVOL class. [1]
GLOBAL	Global access checking table entry. [1]
GMBR	Member class for GLOBAL class (not for use on RACF commands).
GSDSF	Resource group class for SDSF class. [1]
GTERMINL	Resource group class for TERMINAL class. [1]
JESINPUT	Conditional access support for commands or jobs entered into the system through a JES input device.
JESJOBS	Controlling the submission and cancellation of jobs by job name.
JESSPOOL	Controlling access to job data sets on the JES spool (that is, SYSIN and SYSOUT data sets).
NODES	Controlling the following on z/OS systems: • Whether jobs are allowed to enter the system from other nodes • Whether jobs that enter the system from other nodes have to pass user identification and password verification checks
NODMBR	Member class for NODES class (not for use on RACF commands).
OPERCMDS	Controlling who can issue operator commands. [2]
PMBR	Member class for PROGRAM class (not for use on RACF commands).
PROGRAM	Controlled programs (load modules). [1]
PROPCNTL	Controlling if user ID propagation can occur, and if so, for which user IDs (such as the CICS or IMS™ main task user ID), user ID propagation is *not* to occur.
PSFMPL	Used by PSF to perform security functions for printing, such as separator page labeling, data page labeling, and enforcement of the user printable area.
PTKTDATA	PassTicket Key Class enables the security administrator to associate a RACF secured signon secret key with a particular mainframe application that uses RACF for user authentication. Examples of such applications are IMS, CICS, TSO, VM, and APPC.

Table 16. z/OS classes (continued)

Class	Function
RACFVARS	RACF variables. In this class, profile names, which start with & (ampersand), act as RACF variables that can be specified in profile names in other RACF general resource classes.
RVARSMBR	Member class for RACFVARS (not for use on RACF commands).
SCDMBR	Member class for SECDATA class (not for use on RACF commands).
SDSF	Controls the use of authorized commands in the System Display and Search Facility (SDSF). See also GSDSF class.
SECDATA	Security classification of users and data (security levels and security categories). [1]
SECLABEL	If security labels are used, and, if so, their definitions. [2]
SMESSAGE	Controlling to which users a user can send messages (TSO only).
SOMDOBJS	Controlling the client's ability to invoke the method in the class.
SURROGAT	If surrogate submission is allowed, and if allowed, which user IDs can act as surrogates.
TAPEVOL	Tape volumes.
TEMPDSN	Controlling who can access residual temporary data sets. You cannot create profiles in this resource class.
TERMINAL	Terminals (TSO or VM). See also GTERMINL class.
VTAMAPPL	Controlling who can open ACBs from non-APF authorized programs.
WRITER	Controlling the use of JES writers.

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 SETROPTS or, if you do, the GLOBAL checking is not performed.

Table 17. CICS classes

Class	Function
ACICSPCT	CICS program control table. [2]
BCICSPCT	Resource group class for ACICSPCT class. [1]
CCICSCMD	Used by CICS/ESA 3.1, or later, to verify that a user is permitted to use CICS system programmer commands such as INQUIRE, SET, PERFORM, and COLLECT. [1]
DCICSDCT	CICS destination control table. [2]
ECICSDCT	Resource group class for DCICSDCT class. [1]
FCICSFCT	CICS file control table. [2]
GCICSTRN	Resource group class for TCICSTRN class. [2]
HCICSFCT	Resource group class for FCICSFCT class. [1]
JCICSJCT	CICS journal control table. [2]
KCICSJCT	Resource group class for JCICSJCT class. [1]
MCICSPPT	CICS processing program table. [2]
NCICSPPT	Resource group class for MCICSPPT class. [1]
PCICSPSB	CICS program specification blocks or PSBs
QCICSPSB	Resource group class for PCICSPSB class. [1]
SCICSTST	CICS temporary storage table. [2]
TCICSTRN	CICS transactions.
UCICSTST	Resource group class for SCICSTST class. [1]
VCICSCMD	Resource group class for the CCICSCMD class. [1]

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 SETROPTS or, if you do, the GLOBAL checking is not performed.

Table 18. MVS/DFP and DFSMS/MVS classes

Class	Function
MGMTCLAS	SMS management classes.
STORCLAS	SMS storage classes.

Table 19. IMS classes

Class	Function
AIMS	Application group names (AGN).
CIMS	Command.
DIMS	Grouping class for Command.
FIMS	Field (in data segment).
GIMS	Grouping class for transaction.
HIMS	Grouping class for field.
OIMS	Other.
PIMS	Database.
QIMS	Grouping class for database.
SIMS	Segment (in database).
TIMS	Transaction (trancode).
UIMS	Grouping class for segment.
WIMS	Grouping class for other.

Note:

1. You cannot specify this class name on the GENCMD, GENERIC, and GLOBAL/NOGLOBAL operands of the SETROPTS command.

Table 20. Information Management classes

Class	Function
GINFOMAN	Resource group class for Information Management Version 5.
INFOMAN	Member class for Information Management Version 5.

Note:

1. You cannot specify this class name on the GENCMD, GENERIC, and GLOBAL/NOGLOBAL operands of the SETROPTS command.

Table 21. LFS/ESA classes

Class	Function
LFSCLASS	Controls access to file services provided by LFS/ESA.

Table 22. MQM MVS/ESA classes

Class	Function
GMQADMIN	Grouping class for MQM administrative options. [1]
GMQCHAN	Reserved for MQM/ESA.
GMQNLIST	Grouping class for MQM namelists. [1]
GMQPROC	Grouping class for MQM processes. [1]
GMQQUEUE	Grouping class for MQM queues. [1]
MQADMIN	Protects MQM administrative options.
MQCMDS	Protects MQM commands.
MQCONN	Protects MQM connections.
MQNLIST	Protects MQM namelists.

Table 22. MQM MVS/ESA classes (continued)

Class	Function
MQPROC	Protects MQM processes.
MQQUEUE	Protects MQM queues.

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 SETROPTS or, if you do, the GLOBAL checking is not performed.

Table 23. NetView classes

Class	Function
NVASAPDT	NetView/Access Services.
PTKTVAL	Used by NetView/Access Services Secured Single Signon to store information needed when generating a PassTicket.
RMTOPS	NetView® Remote Operations.
RODMMGR	NetView Resource Object Data Manager (RODM).

Table 24. z/OS UNIX System Services classes

Class	Function
DIRACC	Controls auditing (via SETROPTS LOGOPTIONS) for access checks for read/write access to HFS directories. Profiles are not allowed in this class.
DIRSRCH	Controls auditing (via SETROPTS LOGOPTIONS) of HFS directory searches. Profiles are not allowed in this class.
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.
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.

Table 25. TSO classes

Class	Function
ACCTNUM	TSO account numbers.
PERFGRP	TSO performance groups.
TSOAUTH	TSO user authorities such as OPER and MOUNT.
TSOPROC	TSO logon procedures.

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.

Class	Purpose
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.
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.
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.

Class	Purpose
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.

Appendix F. Using RACFISPF

Attention

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

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. To establish a RACFISPF environment, enter:

```
racfispf
```

To end the RACFISPF environment at any time, enter:

```
end
```

Note: RACF does not require that you enter a password to establish a RACFISPF environment. However, your installation may. If your installation requires a password, RACFISPF prompts you for your logon password. After you have entered your password, you can enter valid RACF commands.

If you choose to change your password at this time, and are then denied access because your installation has restricted usage of RACF command sessions, your password change is still in effect.

If you have a password phrase assigned to you, you can use (and change) it at the prompt as well.

For more information on RACFISPF, see *z/VM: RACF Security Server Command Language Reference*

Notices

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

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
Armonk, NY 10504-1785
U.S.A.

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

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

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

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

Any references in this information to non-IBM 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 supply in any way it believes appropriate without incurring any obligation to you.

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

IBM Corporation
Site Counsel
2455 South Road
Poughkeepsie, NY 12601-5400
U.S.A.

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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

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

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 the names and addresses used by an actual business enterprise 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.

Privacy Policy Considerations

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 IBM Online Privacy Policy at http://www.ibm.com/privacy and the IBM Online Privacy Statement at http://www.ibm.com/privacy/details, in particular the section entitled “Cookies, Web Beacons and Other Technologies”, and the IBM Software Products and Software-as-a-Service Privacy Statement at http://www.ibm.com/software/info/product-privacy.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at IBM copyright and trademark information - United States (www.ibm.com/legal/us/en/copytrade.shtml).

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

Glossary

For a list of z/VM terms and their definitions, see *z/VM: Glossary*.

The z/VM glossary is also available through the online z/VM HELP Facility, if HELP files are installed on your z/VM system. For example, to display the definition of the term "dedicated device", issue the following HELP command:

```
help glossary dedicated device
```

While you are in the glossary help file, you can do additional searches:

- To display the definition of a new term, type a new HELP command on the command line:

  ```
  help glossary newterm
  ```

  This command opens a new help file inside the previous help file. You can repeat this process many times. The status area in the lower right corner of the screen shows how many help files you have open. To close the current file, press the Quit key (PF3/F3). To exit from the HELP Facility, press the Return key (PF4/F4).
- To search for a word, phrase, or character string, type it on the command line and press the Clocate key (PF5/F5). To find other occurrences, press the key multiple times.

  The Clocate function searches from the current location to the end of the file. It does not wrap. To search the whole file, press the Top key (PF2/F2) to go to the top of the file before using Clocate.

Bibliography

See the following publications for additional information about z/VM. For abstracts of the z/VM publications, see *z/VM: General Information*, GC24-6193.

Where to Get z/VM Information

z/VM product information is available from the following sources:

- IBM Knowledge Center z/VM welcome page (www.ibm.com/support/knowledgecenter/SSB27U/welcome)
- IBM Publications Center (www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss)
- *IBM Online Library: z/VM Collection*, SK5T-7054
- IBM: z/VM Internet Library (www.ibm.com/vm/library/)

z/VM Base Library

Overview

- *z/VM: General Information*, GC24-6193
- *z/VM: Glossary*, GC24-6195
- *z/VM: License Information*, GC24-6200

Installation, Migration, and Service

- *z/VM: Installation Guide*, GC24-6246
- *z/VM: Migration Guide*, GC24-6201
- *z/VM: Service Guide*, GC24-6247
- *z/VM: VMSES/E Introduction and Reference*, GC24-6243

Planning and Administration

- *z/VM: CMS File Pool Planning, Administration, and Operation*, SC24-6167
- *z/VM: CMS Planning and Administration*, SC24-6171
- *z/VM: Connectivity*, SC24-6174
- *z/VM: CP Planning and Administration*, SC24-6178
- *z/VM: Enabling z/VM for OpenStack (Support for OpenStack Icehouse Release)*, SC24-6248
- *z/VM: Enabling z/VM for OpenStack (Support for OpenStack Juno Release)*, SC24-6249
- *z/VM: Enabling z/VM for OpenStack (Support for OpenStack Kilo Release)*, SC24-6250
- *z/VM: Getting Started with Linux on System z*, SC24-6194
- *z/VM: Group Control System*, SC24-6196
- *z/VM: I/O Configuration*, SC24-6198
- *z/VM: Running Guest Operating Systems*, SC24-6228
- *z/VM: Saved Segments Planning and Administration*, SC24-6229
- *z/VM: Secure Configuration Guide*, SC24-6230
- *z/VM: TCP/IP LDAP Administration Guide*, SC24-6236
- *z/VM: TCP/IP Planning and Customization*, SC24-6238
- *z/OS and z/VM: Hardware Configuration Manager User's Guide*, SC33-7989

Customization and Tuning

- *z/VM: CP Exit Customization*, SC24-6176
- *z/VM: Performance*, SC24-6208

Operation and Use

- *z/VM: CMS Commands and Utilities Reference*, SC24-6166
- *z/VM: CMS Pipelines Reference*, SC24-6169
- *z/VM: CMS Pipelines User's Guide*, SC24-6170
- *z/VM: CMS Primer*, SC24-6172
- *z/VM: CMS User's Guide*, SC24-6173
- *z/VM: CP Commands and Utilities Reference*, SC24-6175
- *z/VM: System Operation*, SC24-6233
- *z/VM: TCP/IP User's Guide*, SC24-6240
- *z/VM: Virtual Machine Operation*, SC24-6241
- *z/VM: XEDIT Commands and Macros Reference*, SC24-6244
- *z/VM: XEDIT User's Guide*, SC24-6245

Application Programming

- *z/VM: CMS Application Development Guide*, SC24-6162
- *z/VM: CMS Application Development Guide for Assembler*, SC24-6163
- *z/VM: CMS Application Multitasking*, SC24-6164
- *z/VM: CMS Callable Services Reference*, SC24-6165

- *z/VM: CMS Macros and Functions Reference*, SC24-6168
- *z/VM: CP Programming Services*, SC24-6179
- *z/VM: CPI Communications User's Guide*, SC24-6180
- *z/VM: Enterprise Systems Architecture/Extended Configuration Principles of Operation*, SC24-6192
- *z/VM: Language Environment User's Guide*, SC24-6199
- *z/VM: OpenExtensions Advanced Application Programming Tools*, SC24-6202
- *z/VM: OpenExtensions Callable Services Reference*, SC24-6203
- *z/VM: OpenExtensions Commands Reference*, SC24-6204
- *z/VM: OpenExtensions POSIX Conformance Document*, GC24-6205
- *z/VM: OpenExtensions User's Guide*, SC24-6206
- *z/VM: Program Management Binder for CMS*, SC24-6211
- *z/VM: Reusable Server Kernel Programmer's Guide and Reference*, SC24-6220
- *z/VM: REXX/VM Reference*, SC24-6221
- *z/VM: REXX/VM User's Guide*, SC24-6222
- *z/VM: Systems Management Application Programming*, SC24-6234
- *z/VM: TCP/IP Programmer's Reference*, SC24-6239
- *Common Programming Interface Communications Reference*, SC26-4399
- *Common Programming Interface Resource Recovery Reference*, SC31-6821
- *z/OS: IBM Tivoli Directory Server Plug-in Reference for z/OS*, SA76-0148
- *z/OS: Language Environment Concepts Guide*, SA22-7567
- *z/OS: Language Environment Debugging Guide*, GA22-7560
- *z/OS: Language Environment Programming Guide*, SA22-7561
- *z/OS: Language Environment Programming Reference*, SA22-7562
- *z/OS: Language Environment Run-Time Messages*, SA22-7566
- *z/OS: Language Environment Writing Interlanguage Communication Applications*, SA22-7563
- *z/OS MVS Program Management: Advanced Facilities*, SA22-7644
- *z/OS MVS Program Management: User's Guide and Reference*, SA22-7643

Diagnosis

- *z/VM: CMS and REXX/VM Messages and Codes*, GC24-6161
- *z/VM: CP Messages and Codes*, GC24-6177
- *z/VM: Diagnosis Guide*, GC24-6187
- *z/VM: Dump Viewing Facility*, GC24-6191
- *z/VM: Other Components Messages and Codes*, GC24-6207
- *z/VM: TCP/IP Diagnosis Guide*, GC24-6235
- *z/VM: TCP/IP Messages and Codes*, GC24-6237
- *z/VM: VM Dump Tool*, GC24-6242
- *z/OS and z/VM: Hardware Configuration Definition Messages*, SC33-7986

z/VM Facilities and Features

Data Facility Storage Management Subsystem for VM

- *z/VM: DFSMS/VM Customization*, SC24-6181
- *z/VM: DFSMS/VM Diagnosis Guide*, GC24-6182
- *z/VM: DFSMS/VM Messages and Codes*, GC24-6183
- *z/VM: DFSMS/VM Planning Guide*, SC24-6184
- *z/VM: DFSMS/VM Removable Media Services*, SC24-6185
- *z/VM: DFSMS/VM Storage Administration*, SC24-6186

Directory Maintenance Facility for z/VM

- *z/VM: Directory Maintenance Facility Commands Reference*, SC24-6188
- *z/VM: Directory Maintenance Facility Messages*, GC24-6189
- *z/VM: Directory Maintenance Facility Tailoring and Administration Guide*, SC24-6190

Open Systems Adapter/Support Facility

- *z Systems: Open Systems Adapter-Express Customer's Guide and Reference*, SA22-7935
- *System z9 and eServer zSeries 890 and 990: Open Systems Adapter-Express Integrated Console Controller User's Guide*, SA22-7990
- *System z: Open Systems Adapter-Express Integrated Console Controller 3215 Support*, SA23-2247

- *System z10: Open Systems Adapter-Express3 Integrated Console Controller Dual-Port User's Guide*, SA23-2266

Performance Toolkit for VM

- *z/VM: Performance Toolkit Guide*, SC24-6209
- *z/VM: Performance Toolkit Reference*, SC24-6210

RACF Security Server for z/VM

- *z/VM: RACF Security Server Auditor's Guide*, SC24-6212
- *z/VM: RACF Security Server Command Language Reference*, SC24-6213
- *z/VM: RACF Security Server Diagnosis Guide*, GC24-6214
- *z/VM: RACF Security Server General User's Guide*, SC24-6215
- *z/VM: RACF Security Server Macros and Interfaces*, SC24-6216
- *z/VM: RACF Security Server Messages and Codes*, GC24-6217
- *z/VM: RACF Security Server Security Administrator's Guide*, SC24-6218
- *z/VM: RACF Security Server System Programmer's Guide*, SC24-6219
- *z/VM: Security Server RACROUTE Macro Reference*, SC24-6231

Remote Spooling Communications Subsystem Networking for z/VM

- *z/VM: RSCS Networking Diagnosis*, GC24-6223
- *z/VM: RSCS Networking Exit Customization*, SC24-6224
- *z/VM: RSCS Networking Messages and Codes*, GC24-6225
- *z/VM: RSCS Networking Operation and Use*, SC24-6226
- *z/VM: RSCS Networking Planning and Configuration*, SC24-6227

Prerequisite Products

Device Support Facilities

- *Device Support Facilities: User's Guide and Reference*, GC35-0033

Environmental Record Editing and Printing Program

- *Environmental Record Editing and Printing Program (EREP): Reference*, GC35-0152
- *Environmental Record Editing and Printing Program (EREP): User's Guide*, GC35-0151

Index

A

B

C

D

E

F

G

O

P

Q

R

S

T

U

V

W

Y

Z

Product Number: 5741-A07

Printed in USA

SC24-6215-01