z/VM
7.4

RACF Security Server Auditor's Guide

SC24-6305-74

Note:

Before you use this information and the product it supports, read the information in “Notices” on page 133.

This edition applies to version 7, release 4 of IBM® z/VM® (product number 5741-A09) and to all subsequent releases and modifications until otherwise indicated in new editions.

Last updated: 2024-09-18

© Copyright International Business Machines Corporation 1993, 2024.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures vii

Tables xi

About This Document xiii
Intended Audience xiii
Where to Find More Information xiii
Links to Other Documents and Websites xiii

How to provide feedback to IBM xv

Summary of Changes for z/VM: RACF Security Server Auditor's Guide xvii
SC24-6305-74, z/VM 7.4 (September 2024) xvii
SC24-6305-73, z/VM 7.3 (December 2023) xvii
SC24-6305-73, z/VM 7.3 (September 2022) xvii
SC24-6305-01, z/VM 7.2 (September 2020) xvii

Chapter 1. The RACF Auditor 1
The AUDITOR, group-AUDITOR, and ROAUDIT Attributes 1
Access Control and Accountability 1
Logging 2
Owner-Controlled Logging 2
Auditor-Controlled Logging 3
Using the RACF Cross-Reference Utility Program (IRRUT100) 4
Using the RACF Database Unload Utility Program (IRRDBU00) 4
Using the RACF SMF Data Unload Utility (RACFADU) 5
Using the RACF Report Writer 5
Conducting the Audit 5
Preliminary Information 6
System Information 6
RACF Implementation 7

Chapter 2. Setting Audit Controls 11
General Audit Controls 11
Logging of RACF Commands and RACROUTE REQUEST=DEFINE Requests 12
Bypassing Logging of Activity of Users with the SPECIAL Attribute 12
Logging the Activities of Users with the OPERATIONS Attribute 13
Bypassing Logging of RACF Command Violations 13
Activating Auditing for Security Levels 13
Activating Auditing for Access Attempts by Class 14
Activating Auditing for Security Labels 15
Refreshing In-Storage Generic Profiles 15
Shared System Considerations 16
Examples for Setting Audit Controls Using SETROPTS 16
Specific Audit Controls 17
User Controls 18
General Resource Controls 18
Listing Specific Audit Controls 19
Auditing Events on z/VM 20

Auditing for OpenExtensions VM ... 39
Processing Audit Records on z/VM ... 41
Maintaining Auditability for Shared User IDs on z/VM ... 45

Chapter 3. RACF SMF Data Unload Utility (RACFADU) ... 49
Using the RACF SMF Data Unload Utility ... 49
RACFADU Setup ... 49
Panel Invocation of RACFADU ... 50
Command Invocation of RACFADU ... 51
RACF SMF Data Unload Utility Messages ... 52
Using the Output from the SMF Data Unload Utility ... 52
Sort/Merge Programs ... 52
Relational Databases ... 52
XML ... 52
Using the SMF Data Unload Utility Output with SQL/DS ... 52
Using the RACF SMF data unload utility to generate XML documents ... 57
XML overview ... 57
Producing XML output ... 58
How the XML tag names are derived ... 58
Viewing and working with XML audit reports ... 60
Event Code Qualifiers ... 60

Chapter 4. The Data Security Monitor (DSMON) ... 75
The DSMON Program ... 75
How to Run DSMON ... 75
DSMON Control Statements ... 76
Functions DSMON Uses ... 77
DSMON Reports ... 78
System Report ... 78
Column Headings ... 78
Report Messages ... 79
RACF Group Tree Report ... 79
RACF Class-Descriptor Table Report ... 80
Sample RACF Class-Descriptor Table Report ... 82
RACF Exits Report ... 83
Sample RACF Exits Report ... 84
RACF Global Access-Checking Table Report ... 84
Sample RACF Global Access-Checking Table Report ... 85
Selected User-Attribute Report ... 86
Sample Selected User-Attribute Report ... 88
Sample Selected User-Attribute Summary Report ... 88
Selected Data-Sets Report ... 89
Sample Selected Data-Sets Report ... 90

Appendix A. The RACF Report Writer ... 91
How the RACF Report Writer Operates ... 91
Phase 1 ... 92
Phase 2 ... 93
Phase 3 ... 93
RACF Report Writer Command and Subcommands ... 94
Planning Considerations ... 95
RACF Report Writer Return Codes ... 95
Useful Hints ... 95
RACFRW Command ... 96
RACFRW Subcommands ... 97
SELECT Subcommand ... 97
EVENT Subcommand ... 101

LIST Subcommand....105
SUMMARY Subcommand....107
END Subcommand....108
Using the RACF Report Writer....108
Monitoring Password Violation Levels....109
Monitoring Access Attempts in WARNING Mode....110
Monitoring Access Violations....111
Monitoring the Use of RACF Commands....111
Monitoring Specific Users....112
Monitoring SPECIAL Users....112
Monitoring OPERATIONS Users....112
Monitoring Failed Accesses to Resources Protected by a Security Level....113
Monitoring Accesses to Resources Protected by a Security Label....113
RACF Report Writer Examples....114
Example 1—Obtaining a Report for All RACF SMF Records....114
Example 2—Obtaining a Report for Minidisk Violations on z/VM....114
Example 3—Obtaining Multiple Reports the Wrong Way....114
Example 7—Obtaining Multiple Reports the Right Way....116
Sample Reports....116
Sample Report Writer Output for Shared User IDs....129
Sample RACFRW CONTROL Files....130

Notices....133
Trademarks....134
Terms and Conditions for Product Documentation....134
IBM Online Privacy Statement....135

Bibliography....137
Where to Get z/VM Information....137
z/VM Base Library....137
z/VM Facilities and Features....138
Prerequisite Products....140
Related Products....140

Index....141

Figures

1. GLOBALAUDIT Operand on the RALTER Command....18

2. Output from RLIST VMXEVENT EVENTS Command....23

3. Sample Output from the SETEVENT LIST Command for z/VM (Part 1 of 8)....27

4. Sample Output from the SETEVENT LIST Command for z/VM (Part 2 of 8)....28

5. Sample Output from the SETEVENT LIST Command for z/VM (Part 3 of 8)....29

6. Sample Output from the SETEVENT LIST Command for z/VM (Part 4 of 8)....30

7. Sample Output from the SETEVENT LIST Command for z/VM (Part 5 of 8)....31

8. Sample Output from the SETEVENT LIST Command for z/VM (Part 6 of 8)....32

9. Sample Output from the SETEVENT LIST Command for z/VM (Part 7 of 8)....33

10. Sample Output from the SETEVENT LIST Command for z/VM (Part 8 of 8)....34

11. Creating Audit Records....42

12. Input Panel for RACFADU....50

13. Sample SQL Utility Statements Creating a Table....54

14. SQL/DS Utility Statements Required to Load the Tables....54

15. Sample System Report (z/VM)....79

16. Sample Group-Tree Report....80

17. Class-Descriptor Table Report (Part 1 of 2)....82

18. Class-Descriptor Table Report (Part 2 of 2)....83

19. Sample RACF Exits Report....84

20. Sample RACF Global Access-Checking Table Report (Part 1 of 2)....85

21. Sample RACF Global Access-Checking Table Report (Part 2 of 2)....86

22. Sample Selected User-Attribute Report....88

23. Selected User-Attribute Summary Report....89

24. Sample Selected Data-Sets Report..... 90

25. RACF Report Writer Overview..... 92

26. Key to Symbols in Command Definitions..... 96

27. Summary Activity Report from SMF..... 118

28. Standard Header Page (Part 1 of 3)..... 118

29. Standard Header Page (Part 2 of 3)..... 119

30. Standard Header Page (Part 3 of 3)..... 120

31. General Summary Report..... 120

32. Listing of Status Records..... 121

33. Listing of Process Records..... 122

34. Short User Summary Report..... 123

35. Short Group Summary Report..... 123

36. Short Resource Summary Report..... 123

37. Short Command Summary Report..... 124

38. Short Event Summary Report..... 124

39. Short Owner Summary Report..... 125

40. User by Resource Summary Report..... 125

41. Group by Resource Summary Report..... 125

42. Resource by User Summary Report..... 126

43. Resource by Group Summary Report..... 126

44. Resource by Event Summary Report..... 127

45. Event by Resource Summary Report..... 127

46. Command by User Summary Report..... 128

47. Command by Group Summary Report..... 128

48. Command by Resource Summary Report..... 129

49. Owner by Resource Summary Report..... 129

50. Shared ID Sample Report 1..... 130

51. Shared ID Sample Report 2..... 130

52. Shared ID Sample Report 3..... 130

Tables

1. Correlation of SQL/DS Table Names and Record Types..... 55

2. XML naming exceptions..... 59

3. XML interpretation of special characters example..... 59

4. XML special characters substitutions..... 59

5. Reports Specified by the FUNCTION Control Statement..... 77

6. Reports Specified by the USEROPT Control Statement..... 78

7. Summary of RACFRW Command and Its Operands..... 94

8. Summary of RACFRW Subcommands..... 94

9. EVENT Subcommand Operand Combination Table..... 103

About This Document

This document describes how to use the auditor functions of the IBM RACF® Security Server for z/VM.

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

Intended Audience

This document is intended for those individuals defined as RACF auditors (persons who have the AUDITOR, group-AUDITOR, or ROAUDIT user attribute).

The reader of this document should be familiar with both RACF and any systems that share the same RACF database.

Where to Find More Information

For information about related publications, refer to the "Bibliography" on page 137.

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.

© Copyright IBM Corp. 1993, 2024

How to provide feedback to IBM

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

© Copyright IBM Corp. 1993, 2024

Summary of Changes for z/VM: RACF Security Server Auditor's Guide

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

SC24-6305-74, z/VM 7.4 (September 2024)

This edition supports the general availability of z/VM 7.4. Note that the publication number suffix (-74) indicates the z/VM release to which this edition applies.

SC24-6305-73, z/VM 7.3 (December 2023)

This edition includes terminology, maintenance, and editorial changes.

SC24-6305-73, z/VM 7.3 (September 2022)

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

[7.3] RACF support for z/VM 7.3

Select RACF utilities for database installation, maintenance, and operations along with select RACF reports are now allowed to run if the RACF service machine's 490 minidisk was IPLed; IPLing CMS is no longer required. In addition, The **RACUT100**, **RACUT200**, and **RACFCONV** utilities require the IPL of the 490 minidisk to support reserve and release of the RACF database.

The following topics have been updated:

- “Command and Subcommand Processing:” on page 92
- “RACFADU Setup” on page 49

SC24-6305-01, z/VM 7.2 (September 2020)

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

© Copyright IBM Corp. 1993, 2024

Chapter 1. The RACF Auditor

RACF is a flexible security tool; it allows an installation to set its own security objectives and use RACF to help achieve those objectives in a way that best meets the installation's needs.

Whereas installations might have slightly different security needs, certain RACF user roles or tasks are common to all users. And, at any installation, different users have different levels of responsibility for security or different needs to access resources. Some people might have extensive responsibility for security, whereas others might have little or none; some users might require almost unlimited access to resources, whereas others might need only limited access, and some might be barred from entering the system at all.

The primary means of defining a user's responsibility for security is the RACF *user attribute*. A user attribute is, simply, a part of the RACF definition of what an installation allows a particular user to do. The SPECIAL attribute, for example, is normally assigned to the RACF security administrator; a SPECIAL user can execute any RACF command except those reserved for a user with the AUDITOR attribute.

This separation of powers is necessary because it is the security administrator's job to establish RACF controls; it is the auditor's job to test the adequacy and effectiveness of these controls. In this sense, your job as the auditor is very similar to the job of a financial auditor in a bank.

The AUDITOR, group-AUDITOR, and ROAUDIT Attributes

Once a SPECIAL user assigns the AUDITOR or ROAUDIT user attribute to you, your responsibility is to verify that RACF is meeting your installation's security goals. As a RACF auditor, your job is essentially the same, regardless of whether you have the AUDITOR or ROAUDIT attribute (with responsibility for checking RACF controls on a user, or system-wide, level) or the group-AUDITOR attribute (with responsibility for checking RACF controls for a group and its subgroups). Whereas a user with the group-AUDITOR attribute can only monitor the users and resources owned by a specific group and its subgroups, the responsibility is so much like that of a user with the AUDITOR attribute that this document applies to both and notes any specific differences.

The user with the ROAUDIT attribute (read-only auditor) has the same primary responsibility as the user with the AUDITOR attribute, to monitor the system. The difference between the AUDITOR attribute and the ROAUDIT attribute is that a user with the AUDITOR attribute has the ability to monitor the system as well as setting auditing controls. A user with the ROAUDIT attribute can only monitor the system with the existing set of auditing controls.

Access Control and Accountability

As the auditor, you are responsible for checking that RACF is meeting the installation's needs for access control and accountability. Access control means that you can control user accesses to resources and verify that the accesses allowed are appropriate to the particular resource. For example, you might question why a tape librarian had access to a payroll data set. The auditor needs to verify that an installation has a way to maintain accountability. Accountability means that you can trace activities on the protected system to a particular person. Normally, several people should not share a user ID. RACF allows user IDs to be shared without losing accountability.

To help you to audit access control and accountability, RACF provides:

- Logging routines that record the information you require
- Audit control functions that enable you to specify the information RACF is to record (or log)
- The RACF SMF data unload utility, which converts SMF records into a format which can be used by a relational database manager
- The RACF report writer, which generates tailored reports based on the information you have directed RACF to log

© Copyright IBM Corp. 1993, 2024

- The data security monitor (DSMON), which generates reports containing information about the security environment

To specify the audit control functions, use either the RACF ISPF panels or the RACF commands to direct RACF to log any events relevant to your installation's data security program. You can:

- Load the records produced by the RACF SMF data unload utility into a relational database manager for analysis.
- Invoke the RACF report writer to print out the data RACF has logged and use the reports to identify possible security violations or weaknesses in the security mechanism

The data security monitor (DSMON) generates a set of reports that lets you audit the current status of the data security environment for an installation. You can use the information in the reports to compare the actual system characteristics and resource protection levels with the installation's requirements. A user must have the AUDITOR attribute or the ROAUDIT attribute to run DSMON. For more information, see Chapter 4, “The Data Security Monitor (DSMON),” on page 75.

Logging

Logging—the recording of data about specific events—is the key to auditing the use of RACF at your installation. You must ensure that RACF logs the information you need. RACF uses the system management facilities (SMF) to log data about various RACF events. RACF writes SMF records to a CMS file.

Note: Each additional logging activity that you specify increases RACF and SMF processing and, as a result, might have an impact on RACF performance.

RACF *always* logs information about certain events because knowing about these events is essential to an effective data-security mechanism. The events that RACF always logs are:

- Every use of the RVARY or SETROPTS command
- Every time a RACROUTE REQUEST=VERIFY request fails
- Every time the console operator grants access to a resource as part of the failsoft processing performed when RACF is inactive.

RACF *never* logs some events, because knowing about these events is not essential to effective data security. RACF never logs any use of the following RACF commands:

LISTDSD, LISTGRP, LISTUSER, RLIST,
LDIRECT, LFILE, SRFILE, SRDIR, and SEARCH.

In addition to the events that RACF always logs and never logs, other events RACF can *optionally* log. Optional logging is under the control of either a resource-profile owner or the auditor.

Owner-Controlled Logging

Owners of resources can specify, in the resource profile, what types of accesses to log (successes, failures, or both) and what level of access to log (READ, UPDATE, CONTROL, or ALTER). Owners can also specify that no logging is to occur for an access that is a success or failure. Owner-controlled logging is not directly under your control, but you should verify that resource owners request a level of logging that is consistent with the sensitivity of the resource. Furthermore, your installation can use three methods to *override* the logging that an owner specifies in the resource profile.

1. First, you can suppress auditing for all resources in a specific class by specifying LOGOPTIONS(NEVER(*class-name*)) on the SETROPTS command. Likewise, you can activate auditing

for all access attempts for all resources in a specific class by specifying LOGOPTIONS(ALWAYS(*class-name*)). See "Activating Auditing for Access Attempts by Class" on page 14.

2. Second, if you have the AUDITOR attribute, you can specify additional logging that supersedes the owner's logging specification for a specific resource by *adding* audit controls to the resource profile. Note that you cannot *change* the owner's logging specifications for a specific resource profile, only add to them. You can do this for specific resource profiles by specifying the GLOBALAUDIT operand on the ALTDSD, ALTDIR, ALTFILE, or RALTER command. Using these controls is described in "General Resource Controls" on page 18.
3. Third, your installation can bypass a profile owner's logging specification by using the RACROUTE REQUEST=AUTH postprocessing exit routine. This exit routine can, for certain accesses, specify unconditional logging or unconditionally suppress logging. For example:
   - An installation might use the exit routine to specify unconditional logging for accesses to a highly classified resource.
   - An installation might suppress logging when the exit routine recognizes READ access to common system resources, such as the S-disk in z/VM.

   You should be aware of any such exit-routine specifications. For more information on using exit routines, see *z/VM: RACF Security Server System Programmer's Guide*.

Note to OpenExtensions Users
You can specify logging options for OpenExtensions BFS files in a manner similar to that used with RACF profiles. For more information, see "Auditing for OpenExtensions VM" on page 39.

Auditor-Controlled Logging

You, the auditor, can direct RACF to log additional events. These events are:

- Changes to any RACF profiles
- All RACF commands that a SPECIAL or group-SPECIAL user issues
- All unauthorized attempts to use RACF commands
- Selected z/VM events, using the SETEVENT command
- All RACF-related activities of specific users
- All accesses to resources (data sets and general resources) that RACF allows because the user has the OPERATIONS or group-OPERATIONS attribute
- All accesses to specific data sets
- All accesses to specific general resources
- All accesses to OpenExtensions BFS files and directories
- All accesses to resources protected by specific profiles in the SECLABEL class
- All accesses to a specified class of resources at an access level indicated on the LOGOPTIONS keyword of the SETROPTS command

You can identify which of these events apply to your installation's security goals and use audit controls to direct RACF to log the events you require.

Choosing between Using RACF Commands and ISPF Panels

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

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

- Entering commands can be faster than displaying many panels in sequence.

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

    ```
    RAC HELP PERMIT
    ```

  - In a RACF command session, enter:

    ```
    HELP PERMIT
    ```

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

    ```
    HELP PERMIT SYNTAX    or    RAC HELP PERMIT SYNTAX
    ```

The *ISPF panels* provide the following advantages:

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

  On z/VM, if your installation uses XEDIT for display in ISPF, you can even save the listings on your A-disk. You can also save the output from a SEARCH (including SRFILE and SRDIR) in a REXX exec.
- The ISPF panels for working with z/VM events provide selection lists. Using the selection lists, you can avoid typing errors when specifying RACF event names.
- The ISPF panels for working with password rules allow you to enter all the password rules on one panel.

Using the RACF Cross-Reference Utility Program (IRRUT100)

If you have the AUDITOR, ROAUDIT, or SPECIAL attribute, you can use the RACF cross-reference utility to find and list occurrences of a user ID or group name in the RACF database.

If you have the group-AUDITOR or group-SPECIAL attribute, you can use these utilities only for a user ID or group that is within your scope of authority.

Before using the RACF cross-reference utility, you should consult with your RACF system programmer. You may need to find out *how* to run the utility, and you also need to find out *when* to run the utility so as to reduce its impact on system operations.

For more information on using this utility, see *z/VM: RACF Security Server System Programmer's Guide*.

Using the RACF Database Unload Utility Program (IRRDBU00)

You can also use the RACF database unload utility to provide flexibility in analyzing RACF profile information. The output from this utility is a sequential file that is a relational representation of a restructured RACF database.

If the output is loaded into a database management system (such as DB2® or SQL/DS), you can issue your own queries. For example, you can find and list occurrences of a user ID or group name in the RACF database. You can list members of a group by name rather than user ID.

Before using the RACF database unload utility, you should consult with your RACF system programmer. You may need to find out *how* to run the utility. Your input database must be in the restructured format and you must have UPDATE authority to it.

For more information on running this utility, see *z/VM: RACF Security Server Macros and Interfaces* and *z/VM: RACF Security Server Security Administrator's Guide*.

Using the RACF SMF Data Unload Utility (RACFADU)

The RACF SMF data unload utility is the IBM-recommended utility for processing RACF audit records. With it, you can create a sequential file from the security relevant audit data. You can use the sequential file in several ways. You can:

- View the file directly
- Use the file as input for installation-written programs
- Manipulate the file with sort/merge utilities

You can also upload the file to a database manager (for example, SQL/DS) to process complex inquiries and create installation-tailored reports.

For details on the RACF SMF data unload utility, see Chapter 3, "RACF SMF Data Unload Utility (RACFADU)," on page 49.

Using the RACF Report Writer

The profile listings that the RACF commands provide can help you to verify the audit controls that exist at any particular time. The RACF report writer helps you to monitor RACF-related activity during system operation and to verify that these activities are consistent with your installation's security goals. The RACF report writer provides printed reports based on the data your audit controls directed RACF to log.

The report writer makes use of certain system management facility (SMF) records to obtain information. You can control the selection of these records and the format and type of report that the report writer produces through the use of the RACFRW command and its subcommands.

However, the report writer supports audit records for RACF 1.9.2 and earlier. It does not support most of the audit records introduced in RACF 1.10 for z/VM or later releases.

See Appendix A, "The RACF Report Writer," on page 91 for a detailed description of the report writer, the RACRPORT EXEC that invokes it, the RACFRW command, and samples of the available reports.

Conducting the Audit

Asking the right questions is an essential part of *any* audit, including an audit of your own RACF-protected installation or a review of another installation. In such a review or audit, your principal review objectives are:

1. To judge how effectively RACF has been implemented to handle security at the installation
2. To identify any security exposures
3. To recommend ways to improve the system.

To accomplish these objectives, you need to understand your installation and its security requirements. To obtain the information, you can interview a few key people such as the security administrator, the system programmer responsible for installing and implementing RACF, and a senior member of the system support group. Asking the right questions of the right people can help you in your audit.

One way to deal with the mass of information used for an audit is to divide it into categories: preliminary information, system information, and RACF information. The rest of this chapter uses these categories to identify blocks of information you need or questions you might ask. Not all of the suggestions apply at any one installation; any particular installation may require additional investigation. Treat these suggestions as a starting point, then tailor and expand your audit to fit the conditions that exist.

When you are conducting an audit, you should obtain current installation reports from the data security monitor (DSMON). These reports are helpful in answering a number of your questions. You can also use the DSMON reports to verify that the *actual* status of various security mechanisms is what you and the installation expect. DSMON is described in Chapter 4, "The Data Security Monitor (DSMON)," on page 75.

Preliminary Information

Before conducting an audit, you should establish preliminary information concerning the type, size, and complexity of your installation. The following questions should help you get started.

1. List the processor complexes and their associated system control programs (SCPs), as well as the release and level of RACF for each. You can use the DSMON reports to answer this particular question.
2. Are processor complexes linked (for example, by NJE, RSCS, JES2, or JES3)?
3. Are you using multiple RACF service machines?
4. Do you have dial-up lines?
5. Explain briefly the classification system.
6. What is the highest classification of data processed and/or transmitted?

System Information

An operating system should have integrity; that is, it should prevent one program from interfering with or modifying the execution of another system or user program unless the interference is authorized. To increase your awareness of potential security problems, read related publications that provide overview information and describe system features that promote security. A list of the related publications is provided in the preface of this book.

Basic System

Use the following questions to help establish foundation information concerning your system.

1. What is the operating system version, release level, and service level (RSU)? You can use the DSMON reports to answer this particular question.
2. How many local modifications have been applied (excluding exit routines)?
3. What are the main areas and/or functions modified?
4. Are the systems the same on all processor complexes?
5. What exit routines are in the system and what is their purpose? Could these exit routines affect RACF protection?

System Protection

Use the following questions to ascertain current system protection.

1. How are changes to the system controlled and documented?
2. Are the system disks protected?
3. Are key security items, (such as RACF databases, CP directory, password data, SMF data, source and load modules for RACF exit routines, and SMF routines) all identified and protected? You can use the DSMON reports to answer this particular question.

Miscellaneous

The following questions do not fall into any of the preceding categories; however, the information gained from the answers could be useful when conducting an audit.

1. If dial-up terminals are used, how is unauthorized use prevented?
2. How far back do system backup dumps go?
3. Are all IPLs logged and the reasons reported?
4. Is all time on the system accounted for?
5. Is it possible to detect if the system has been loaded without RACF? You can use the DSMON reports to answer this particular question.
6. How is the use of RACF commands (such as RVARY) controlled?

RACF Implementation

Installing RACF does not necessarily mean that the RACF security facilities were correctly implemented and are being correctly maintained. (For more information about implementing RACF, see *z/VM: RACF Security Server Security Administrator's Guide*.)

Protection Plan

You should ask the following questions to determine what resources your installation is currently protecting.

1. How many RACF users and groups do you have? All or part of this question can be answered by using the DSMON reports.
2. Do you have any non-RACF users? If so, why?
3. Which of the following resources are RACF-protected, what proportion of each is protected, and how is it decided which to protect? All or part of this question can be answered by manipulating the output of the RACF database unload utility.

   Tape volumes
   Minidisks
   SFS files
   SFS directories
   Appropriate CP commands, diagnosis and functions
   Nodes
   Unit record devices
   Terminals
   Shared user IDs
   z/VM readers
   Ability to use the alternate user ID (that is, VMBATCH)
   Key resources unique to the installation
   Guest LANs
   virtual switches
4. How does the installation ensure that appropriate protection is maintained?
5. What protection is available for resources *not* protected by RACF?
6. Is the protection policy reasonable?

Usage

The following questions will help determine how RACF is currently being implemented.

1. Which user IDs have any of the following privileged attributes or authorities? Why? You can use the DSMON reports to answer this particular question.

   SPECIAL and group-SPECIAL
   OPERATIONS and group-OPERATIONS
   AUDITOR and group-AUDITOR
   ROAUDIT
   CLAUTH
   JOIN
   CONNECT
2. How is the granting of these privileges controlled?
3. Are user IDs shared? If so, why, and how is accountability maintained?
4. Is the default for UACC always NONE? If not, why?

All or part of this question can be answered by manipulating the output of the RACF database unload utility.

5. How are password qualities complied with? Do you use, for example, password length, nature (alphabetic, alphanumeric, no vowels), repetition, or change frequency?
6. What RACF information, such as the following, is logged to SMF?

   Command violations
   Changes to profiles
   Accesses to specific resources
   Actions of SPECIAL and group-SPECIAL users
   Actions of OPERATIONS and group-OPERATIONS users
7. Who decides what resource-access information is to be collected? On what criteria?
8. What RACF statistics are collected?
9. What are the access rules when RACF is inactive or unavailable, such as stopping production, performing repair work only, or allowing selected jobs and applications to run?
10. Is WARNING mode active, entirely or partially? Are there non-WARNING mode resources?

    All or part of this question can be answered by manipulating the output of the RACF database unload utility.
11. Do access lists contain groups rather than individuals?
12. How is the authority to run production work handled? Does the job submitter have access to production data? If so, how are the profiles deleted?
13. How is RACF protection handled in disaster-recovery plans?
14. Describe any operational or usage problems for which the installation cannot currently determine a solution.
15. How are the SYSSEC macro options set?

Technical

The following questions will provide technical orientation.

1. What RACF exit routines are used, and what functions do they perform? The following list identifies the exits. You can use the DSMON reports to answer this particular question.

   ICHDEX01
   (password encoding)

   ICHRIX01
   (RACROUTE REQUEST=VERIFY request preprocessing)

   ICHRIX02
   (RACROUTE REQUEST=VERIFY request postprocessing)

   ICHRCX01
   (RACROUTE REQUEST=AUTH request preprocessing)

   ICHRCX02
   (RACROUTE REQUEST=AUTH request postprocessing)

   ICHRDX01
   (RACROUTE REQUEST=DEFINE request preprocessing)

   ICHRDX02
   (RACROUTE REQUEST=DEFINE request postprocessing)

   ICHCCX00
   (command preprocessing)

   ICHCNX00
   (command preprocessing)

ICHRFX01
(RACROUTE REQUEST=FASTAUTH request preprocessing)

ICHRFX02
(RACROUTE REQUEST=FASTAUTH request postprocessing)

ICHPWX01
(new password)

ICHPWX11
(new password phrase)

ICHRLX01
(RACROUTE REQUEST=LIST request pre/postprocessing)

ICHRLX02
(RACROUTE REQUEST=LIST request selection)

ICHRSMFE
(report writer)

2. How are the exit-routine functions and changes authorized and controlled?
3. Who is allowed to update exit-routine code (both source and load form)?
4. What SETROPTS options are used? Are any important protection or monitoring functions set off?
5. Have basic RACF facilities been enhanced, excluding exit-routine code?
6. How many primary RACF databases are there? You can use the DSMON reports to answer this particular question.
7. Does each primary RACF database have a backup on a different volume? You can use the DSMON reports to answer this particular question.
8. What other backup facilities exist for RACF databases?
9. How is the RACF database synchronized after a restore?
10. Are all RACF databases adequately protected, and who has access to them? You can use the DSMON reports to answer this particular question.
11. How does the installation control the switching and deactivating of the RACF databases (RVARY command, IPL/database name table)?
12. Are any special checks required on the use of PERMIT?
13. How are passwords protected against disclosure when batch jobs are submitted through internal readers?
14. How are restores of entire volumes handled? How are synchronization problems between volumes and the RACF databases resolved?
15. What are the RACF class names as defined in the class descriptor table (CDT)? What are the UACCs associated with these names? Can OPERATIONS users access the resources by default? You can use the DSMON reports to answer this particular question.
16. Is there a global access table, and what resources are specified in the table? You can use the DSMON reports to answer this particular question.
17. Is there a global disk table defined in the RACF/CP module HCPRWA?

Administration Control

The following questions will provide information concerning how RACF is administered at your installation.

1. Who is responsible for the administration of RACF? You can use the DSMON reports to answer this particular question.
2. Who is responsible for the technical aspects of RACF?
3. Are data owners identified?
4. Do data owners classify their data?

5. Is the degree of protection provided by the installation based on the owner classification?
6. Are there written and approved procedures for RACF administration?
7. Does the installation maintain written records of requests for changes to RACF protection and the resulting actions taken?
8. How are users and groups administered? How are additions, deletions, changes, connections, and authorities handled?
9. How is the authority to protect resources and grant access checked and handled?
10. How is the granting of temporary authorities handled? Can users issue PERMIT/CONNECT for temporary access, or are there privileged attributes available for emergency use?
11. How is password distribution handled?
12. How are lost passwords handled?
13. Is additional verification required for users with privileged attributes? Are these users restricted to particular terminals?
14. Is there an emergency user ID with the SPECIAL attribute available for use when no other SPECIAL user ID can be used? If so, how does the installation protect the user ID and its password? You can use the DSMON reports to answer this particular question.
15. Is the auditor a different person from the RACF security administrator? What are the responsibilities of the auditor? You can use the DSMON reports to answer this particular question.
16. Is there any user education available?

Management Control

The following questions address management control.

1. What reports are available to users, owners, and installation management to ensure that the system is not being misused? Examples are reports that identify violation attempts, unauthorized access attempts, and unauthorized use of commands and privileges.
2. How frequently are reports produced, and who sees them?
3. If a security violation occurs, what follow-up action does the installation take?
4. Is the installation using DSMON reports to monitor the basic system security environment? If not, why isn't it?

Chapter 2. Setting Audit Controls

Audit controls are special RACF functions that RACF allows only the auditor to perform. To preserve the checks and balances necessary to an effective security mechanism, not even the security administrator with the SPECIAL attribute can execute auditor functions. Therefore, you should ensure that SPECIAL users do not also have the AUDITOR attribute.

Note: Users with the ROAUDIT attribute can only perform the actions to list the specific audit controls that are mentioned in this topic, because the ROAUDIT attribute only enables the user to perform the monitoring tasks of the auditor. The actions to set auditing controls that are mentioned in this topic are not included with the ROAUDIT attribute.

The following list summarizes audit controls you can use

- **General audit controls:**
  - Auditing options specified on the SETROPTS (Set RACF Options) command
  - Auditing z/VM events specified using z/VM event profiles and the SETEVENT (SET z/VM Event) command.
- **Specific audit controls:**
  - All RACF-related activities of specific users
  - Attempts to access data sets protected by specific profiles
  - Attempts to access general resources (such as terminals, minidisks, SFS files, SFS directories, and others) that are protected by specific profiles

General Audit Controls

You specify general (system-wide) audit controls on either the SETROPTS command or the SET AUDIT OPTIONS ISPF panel. General audit controls direct RACF to log (or not to log) certain security-relevant events, such as the activities of OPERATIONS or group-OPERATIONS users, RACF command violations, and attempts to access RACF-protected resources.

To specify the general audit controls, you must have the AUDITOR attribute. After you have initially established your controls or modified existing controls, it is a good practice to list the current options to verify that the controls are correct.

If you have the AUDITOR attribute, you can specify these SETROPTS operands or request the function on the corresponding panel:

AUDIT and NOAUDIT
CMDVIOL and NOCMDVIOL
LIST
LOGOPTIONS
OPERAUDIT and NOOPERAUDIT
REFRESH GENERIC
REFRESH RACLIST
SAUDIT and NOSAUDIT
SECLABELAUDIT and NOSECLABELAUDIT
SECLEVELAUDIT and NOSECLEVELAUDIT

If you are a group-AUDITOR, you can use only the LIST and REFRESH GENERIC operands.

© Copyright IBM Corp. 1993, 2024

Logging of RACF Commands and RACROUTE REQUEST=DEFINE Requests

If you have the AUDITOR attribute, you can specify the classes for which RACF logs all detected accesses to the RACF database through RACF commands and RACROUTE REQUEST=DEFINE requests. You can specify this option with the AUDIT operand on the SETROPTS command; it becomes effective immediately. The following example specifies that you want RACF to log RACF commands and RACROUTE REQUEST=DEFINE requests for users, groups, data sets, and the VMMDISK and TERMINAL general resource classes.

```
SETROPTS  AUDIT(USER  GROUP  DATASET  VMMDISK  TERMINAL)
```

If you specify AUDIT(*), RACF logs RACF command and RACROUTE REQUEST=DEFINE request activity for all classes.

If you want to log any change in RACF protection for IMS, enter:

```
SETROPTS AUDIT(IMS)
```

The following table shows the commands that are audited when SETROPTS AUDIT is active for the specified class. The RACROUTE request refers to a RACROUTE REQUEST=DEFINE request.

USER	GROUP	DATASET	Classes in the CDT	DIRECTRY	FILE
ADDUSER	ADDGROUP	ADDSD	PERMIT	ADDDIR	ADDFILE
ALTUSER	ALTGROUP	ALTDSD	RACROUTE[1]	ALTDIR	ALTFILE
CONNECT	CONNECT	DELDSD	RALTER	DELDIR	DELFILE
DELUSER	DELGROUP	PERMIT	RDEFINE	PERMDIR	PERMFILE
PASSWORD	REMOVE	RACROUTE[1]	RDELETE	RACROUTE[1]	RACROUTE[1]
REMOVE					

Note: SETROPTS AUDIT(USER) includes all successful password and password phrase changes.

If you have the AUDITOR attribute, you can also specify the NOAUDIT operand on the SETROPTS command, and identify the class or classes for which you do not want RACF to log RACF command and RACROUTE REQUEST=DEFINE requests. If you specify NOAUDIT(*), RACF does not log RACF command and RACROUTE REQUEST=DEFINE requests for any class.

NOAUDIT(*) is in effect at RACF initialization.

Note: If you have the AUDITOR attribute, you can specify with the UAUDIT operand on the ALTUSER command that you want RACF to log all RACROUTE REQUEST=AUTH and RACROUTE REQUEST=DEFINE requests issued for the user and all RACF commands (except LISTGRP and LISTUSER) issued by the user.

Bypassing Logging of Activity of Users with the SPECIAL Attribute

If you have the AUDITOR attribute, you can request that RACF bypass logging of all RACF commands and the RACROUTE REQUEST=AUTH and RACROUTE REQUEST=DEFINE requests issued by users with the SPECIAL or group-SPECIAL attribute. You can specify this option with the NOSAUDIT operand on the SETROPTS command as shown in the following example:

```
SETROPTS  NOSAUDIT
```

If you have the AUDITOR attribute, you can also specify the SAUDIT operand on the SETROPTS command to indicate that you want RACF to log the command and request activity of users with the SPECIAL or group-SPECIAL attribute. The exceptions are LISTDSD, LISTGRP, LISTUSER, RLIST, LFILE, LDIRECT, SRFILE, SRDIR, and SEARCH. These are never logged.

[1] RACROUTE refers to a RACROUTE REQUEST=DEFINE request.

Note: If you are concerned only with how SPECIAL users change profiles, you do not need to specify SAUDIT if AUDIT(*) is in effect.

SAUDIT is in effect at RACF initialization.

Logging the Activities of Users with the OPERATIONS Attribute

If you have the AUDITOR attribute, you can audit all accesses to resources granted because the user has the OPERATIONS or group-OPERATIONS attribute, by using the OPERAUDIT operand on the SETROPTS command. The following example shows how to specify this option.

```
SETROPTS  OPERAUDIT
```

If you specify OPERAUDIT, RACF logs all accesses to RACF-protected resources granted because the user has the OPERATIONS or group-OPERATIONS attribute, and all uses of the ADDSD, ADDFILE, ADDDIR, and RDEFINE commands allowed because a user has the OPERATIONS or group-OPERATIONS attribute.

Note: Some programs that call RACF functions such as RACROUTE REQUEST=AUTH and RACROUTE REQUEST=DEFINE can request that RACF perform no logging. Thus, if an OPERATIONS or group-operations user accesses a protected resource through such a program, RACF does not log the access even if you request OPERAUDIT.

OPERAUDIT overrides the audit field of data set, SFS file, SFS directory, and general resource profiles. OPERAUDIT does not affect any auditing requested by the GLOBALAUDIT operand on the RACF commands.

If you have the AUDITOR attribute, you can also specify NOOPERAUDIT. NOOPERAUDIT does no special auditing of users with the OPERATIONS or group-OPERATIONS attribute.

NOOPERAUDIT is in effect at RACF initialization.

Bypassing Logging of RACF Command Violations

If you have the AUDITOR attribute, you can request that RACF bypass logging of all violations detected by RACF commands (except RVARY and SETROPTS, which are always logged) during RACF command processing. You can specify this option with the NOCMDVIOL operand on the SETROPTS command as shown in the following example:

```
SETROPTS  NOCMDVIOL
```

A violation can occur because RACF does not authorize a user to modify a particular profile or to enter a particular operand on a command.

If you have the AUDITOR attribute, you can also specify the CMDVIOL operand on the SETROPTS command. This operand tells RACF to log all command violations. The exceptions are LISTDSD, LISTGRP, LISTUSER, RLIST, LFILE, LDIRECT, SRFILE, SRDIR, and SEARCH. These are never logged.

Note: Specifying CMDVIOL causes RACF to log all the command violations that it detects. You can then use the RACF report writer to produce a printed audit trail of command violations. You can determine how many command violations are occurring and which users are causing the violations. A significant number of command violations, especially when RACF is first installed, may indicate the need for more user education. The report can also help you to identify any specific users who are persistently trying to alter profiles without the proper authority.

CMDVIOL is in effect at RACF initialization.

Activating Auditing for Security Levels

If you have the AUDITOR attribute, you can activate auditing of access attempts to all RACF-protected resources. To activate this option, specify the SECLEVELAUDIT operand with an installation-defined security level name on the SETROPTS command. Auditing is done if the profile protecting a resource is equal to or greater than the security level you specify on the SECLEVELAUDIT operand.

Note that you can only specify a security level name defined by your installation in the SECLEVEL profile in the SECDATA class. If you specify a security level that is not in the SECLEVEL profile for the SECDATA class, RACF ignores the operand and does no logging. Also, the SECDATA class must be active if you want RACF to perform security level control auditing. The following example shows how to activate auditing based on the security level CONFIDENTIAL.

```
SETROPTS  SECLEVELAUDIT(CONFIDENTIAL)
```

When you specify a security level, RACF audits all attempts to access resources with the specified security level and higher. This option allows your installation to audit access attempts to a RACF-protected resource, based on the sensitivity of the resource, as determined by the installation. If you do not specify a security level, RACF audits all access attempts to all resources for which your installation has defined a security level (SECLEVEL).

Note:

1. If a program issues a RACROUTE REQUEST=AUTH or RACROUTE REQUEST=DEFINE request and specifies that RACF should not perform any logging, RACF does not log the event even if you request logging.
2. When RACF grants access to a resource because of an entry in the global access checking table, RACF does not log the event even if you request logging.

If you have the AUDITOR attribute, you can also deactivate auditing of access attempts to RACF-protected resources based on installation-defined security levels. To deactivate this option, specify the NOSECLEVELAUDIT operand on the SETROPTS command.

NOSECLEVELAUDIT is in effect at RACF initialization.

Activating Auditing for Access Attempts by Class

If you have the AUDITOR attribute, you can audit attempts to access resources in specified classes according to the option selected. You can specify the DATASET class and any active classes in the class descriptor table. The resources need not have profiles created in order for the auditing to occur.

The following command specifies that auditing be done for all attempts to access the TERMINAL class.

```
SETROPTS  LOGOPTIONS(ALWAYS(TERMINAL))
```

In this case, auditing is done every time a user logs on at any terminal on the system, whether that terminal is protected by a profile or not, and whether that profile specifies auditing or not.

You can specify that auditing be done for the following conditions:

ALWAYS
All attempts to access resources protected by the class are audited.

NEVER
No attempts to access resources protected by the class are audited. (All auditing is suppressed.)

SUCCESSES
All successful attempts to access resources protected by the class are audited.

FAILURES
All failed attempts to access resources protected by the class are audited.

DEFAULT
Auditing is controlled by the profile protecting the resource, if a profile exists. You can specify DEFAULT for all classes by specifying an asterisk (*) with DEFAULT.

Note:

1. The SUCCESSES and FAILURES operands result in auditing in addition to any auditing specified in profiles in the class. In contrast, the ALWAYS and NEVER operands override any auditing specified in profiles in the class.

2. If LOG=NONE is specified on a RACROUTE REQUEST=AUTH, it will take precedence and auditing is not performed.
3. When RACF grants access to a resource because of an entry in the global access checking table, RACF does not log the event even if you request logging.

LOGOPTIONS(DEFAULT(*)) is in effect at RACF initialization.

To reset logging to be controlled by profiles, specify LOGOPTIONS(DEFAULT(*)) on the SETROPTS command.

Activating Auditing for Security Labels

If you have the AUDITOR attribute, you can audit all attempts to access resources whose profiles have a security label specified. The auditing that is done is specified in the SECLABEL profile that defines the security label. To do this, specify the SETROPTS command as follows:

```
SETROPTS  SECLABELAUDIT
```

When SECLABELAUDIT is in effect, the SECLABEL profiles for which RACLIST processing has been done enhance the auditing specified in resource profiles. For example, when a resource with security label EAGLE is accessed (and when a user with security label EAGLE logs on), RACF records the event if either the in-storage copy of the SECLABEL profile named EAGLE requires it, or the profile protecting the resource requires it.

For example, to audit all failed accesses to resources with a SECLABEL of EAGLE, the installation should issue the following command:

```
RALTER SECLABEL EAGLE AUDIT(FAILURES(READ))
```

After this command has been issued, a DATASET profile that has a security label of EAGLE, but no auditing specified, will have failed access attempts audited due to the SECLABEL auditing specified.

Note: A value of NONE in the SECLABEL profile does not suppress auditing; auditing is determined by other auditing specifications (such as the resource profile).

NOSECLABELAUDIT is in effect at RACF initialization.

To reset this option, specify NOSECLABELAUDIT on the SETROPTS command.

For performance reasons, you need to carefully plan what SECLABELs are audited in the z/VM environment. Also, if you are using the protection of z/VM events with the VMMAC class, be aware that auditing security labels will increase system overhead when CP calls RACF for these events. For more information, see *z/VM: RACF Security Server System Programmer's Guide*.

When auditing security labels with the SECLABELAUDIT function, SMF audit records are written, thus requiring a high amount of system overhead. It is advised that auditing **not** be turned on for every SECLABEL in the system. Only those SECLABELs with specific auditing requirements, as defined by the installation, should be audited.

Refreshing In-Storage Generic Profiles

You may want to use GENERIC REFRESH after changing the logging options in a generic profile that protects a specific resource, as described in “Specific Audit Controls” on page 17. However, extensive use of GENERIC REFRESH can adversely affect system performance.

You can refresh in-storage generic profiles by specifying both the GENERIC and REFRESH operands on the SETROPTS command. When you specify both GENERIC and REFRESH, you also specify one or more classes for which you want RACF to refresh in-storage generic profiles. This causes all the in-storage generic profiles within the specified general resource class (except those in the global access checking table) to be replaced with new copies from the RACF database. The following example shows how to refresh in-storage generic profiles for the DATASET and TERMINAL classes.

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

Note that you must issue this command each time you want RACF to perform the refresh process.

If you specify GENERIC(*), RACF refreshes profile lists for the DATASET class and all active classes in the class descriptor table except group resource classes (such as GTERMINL and GDASDVOL).

When you initiate the refresh procedure, RACF sets an indicator in the RACF communication vector table for the class(es) that you specified. After the indicator is set, RACF refreshes the profile lists the next time it invokes the generic-profile search routine.

Note: The z/VM system does not use either the FRACHECK or RACLIST macro; however, a z/VM user can utilize these through the RACROUTE interface. See *z/VM: Security Server RACROUTE Macro Reference*.

If you specify NOGENERIC on the SETROPTS command, RACF stops using in-storage generic profile lists but does not immediately delete them. On z/VM, RACF deletes the profile lists only when you again specify GENERIC. When you specify GENERIC, RACF rebuilds the profile lists. (If SETROPTS GENLIST has been used on your system, a copy of the generic profiles for the resource resides in the RACF service machine. You can also use REFRESH GENERIC to refresh these in-storage generic profiles.)

Shared System Considerations

In a non-SSI cluster environment, the refresh operation for SETROPTS RACLIST processing applies only to the system on which you issue the SETROPTS command. If your installation has two or more non-cluster systems sharing a RACF database, you must issue the SETROPTS command on all systems to have the refresh done on all systems. However, if you do not perform a refresh (issue the SETROPTS command with the REFRESH option) on a system sharing a RACF database and that system needs to re-IPL, the refresh takes effect on that system when re-IPL is performed.

See “SETROPTS Command Propagation” on page 16 for information on the SETROPTS commands that are automatically propagated in certain system environments.

SETROPTS Command Propagation

If you issue the SETROPTS command with any operand that changes the RACF database or issue the SETROPTS REFRESH command, the command is automatically propagated to all RACF servers that run on the same z/VM system, and to other systems in the same SSI cluster as the issuing system. Only the SETROPTS LIST command is not propagated.

On a system outside an SSI cluster, the action is not propagated to other systems that share the RACF database. You must issue the SETROPTS command separately for each system or restart the RACF servers on the other system or IPL the other system.

Examples for Setting Audit Controls Using SETROPTS

The following examples show how to set system-wide audit controls by using the SETROPTS command.

Note: If you wish to list the current system-wide audit controls set with the SETROPTS command, enter:

```
SETROPTS  LIST
```

You can also use the LIST operand on the SETROPTS command; for example:

```
SETROPTS  SAUDIT  LIST
```

Example 1

To log all RACF commands issued by SPECIAL and group-SPECIAL users, enter:

```
SETROPTS  SAUDIT
```

Example 2

To log all accesses to resources that users make as a result of the OPERATIONS attribute, enter:

```
SETROPTS  OPERAUDIT
```

Example 3

To log all RACF command violations, enter:

```
SETROPTS  CMDVIOL
```

Example 4

To log all attempts to access any resource with a security level of confidential or higher enter:

```
SETROPTS  SECLEVELAUDIT(CONFIDENTIAL)
```

Example 5

To refresh the in-storage profiles for terminals when SETROPTS RACLIST has been used for the terminal class, enter:

```
SETROPTS  REFRESH  RACLIST(TERMINAL)
```

Example 6

To log any changes to the profiles in the VMMDISK, VMRDR, FILE, and DIRECTRY classes, enter:

```
SETROPTS  AUDIT(VMMDISK,VMRDR,FILE,DIRECTRY)
```

Note: You can combine these examples into a single SETROPTS command by entering:

```
SETROPTS  AUDIT(VMMDISK,VMRDR,FILE,DIRECTRY)
      SAUDIT  OPERAUDIT  CMDVIOL  SECLEVELAUDIT(CONFIDENTIAL)
      REFRESH  RACLIST(TERMINAL)
```

Example 7

To log all access to shared user IDs, enter:

```
SETROPTS  LOGOPTIONS(ALWAYS(SURROGAT))
```

Example 8

To enable the use of SECLABEL profiles to determine the desired level of auditing, enter:

```
SETROPTS SECLABELAUDIT
```

Specific Audit Controls

Specific audit controls enable you to log the following:

- All RACF-related activities for specific users
- Attempts to access specific data sets
- Attempts to access specific general resources
- Attempts to access resources protected by a SECLABEL.

You can also list the complete contents of all profiles, including the owner-specified and auditor-specified logging options for resources.

If you have the AUDITOR attribute, you can set specific controls for any user, data set, or general resource, and list the contents of any profile. If you have the group-AUDITOR attribute, you can set

controls and list profile contents only for those users, data sets, and general resources owned by the group in which you have the attribute, and any subgroup of that group.

User Controls

You can use the UAUDIT or NOUAUDIT operand on the ALTUSER command, or request the corresponding functions on the AUDIT USER panel, to log all RACF-related activities for a specific user. When you set this control, RACF logs the following events:

- All RACF commands that the user issues
- All additions, changes, or deletions that the user makes to the RACF profiles or BFS objects
- All attempts that the user makes to access RACF-protected resources, including BFS objects, except those authorized by global access checking.

In general, you would probably not request user audit-logging as a matter of course, but it is useful in special situations. For example, you can specify user-audit logging if you suspect, based on other indicators such as command violations, that a particular user may be misusing the system or persistently trying to access or delete resources outside the user's control. Examples of the type of event that might indicate misuse of the system are either unauthorized attempts to modify a critical system resource (such as the S-disk) or a highly classified user resource (like a payroll or business-planning data).

Example

To use the UAUDIT operand on the ALTUSER command to audit the person whose user ID is SMITH, enter:

```
ALTUSER  SMITH  UAUDIT
```

General Resource Controls

If owner controlled logging does not provide enough information for your audit, you can use the GLOBALAUDIT operand on the RALTER command or request the corresponding function on the AUDIT GENERAL RESOURCE ACCESS panel, in addition to the owner-specified logging values, to log user accesses to general resources. To audit SFS files or directories, you can use the GLOBALAUDIT operand on the ALTFILE or ALTDIR command.

GLOBALAUDIT allows you to specify logging for different kinds of attempts that users make to access resources at a given access level. With GLOBALAUDIT, you can log successful accesses, failed accesses, or both to a given resource and specify READ, UPDATE, CONTROL, or ALTER for the access level to the resource.

Figure 1 on page 18 summarizes the GLOBALAUDIT operand for RALTER and what you are able to specify for logging. (For a complete description of the RALTER command and its operands, see *z/VM: RACF Security Server Command Language Reference*.

```
        [               {   ALL                                     }   ]
        [               {{{ FAILURES }                          }   }   ]
RALTER  [ GLOBALAUDIT ( {{{ NONE     } {(audit-access-level)] } ... } ) ]
        [               {{{ SUCCESS  }                          }   }   ]
```

Figure 1. GLOBALAUDIT Operand on the RALTER Command

As a general rule, you do not audit accesses to most resources. Therefore, GLOBALAUDIT(NONE) is the default for the operand. After you complete your audit of the resource, it is good practice to restore the default. When GLOBALAUDIT(NONE) is in effect, RACF logs accesses to the resource only as specified by the resource owner.

Example

To use the RALTER command to specify auditing of all write attempts to z/VM minidisk CMS.19E, enter:

```
RALTER  VMMDISK  CMS.19E  GLOBALAUDIT(ALL(UPDATE))
```

Listing Specific Audit Controls

RACF provides commands and corresponding ISPF panels that allow RACF users, depending on their authority or attributes, to examine the contents of RACF profiles. You, as auditor, can list the contents of all the RACF profiles (or all the profiles within the scope of your group if you are a group-AUDITOR). You can find a complete description of each of the commands, including sample output, in the *z/VM: RACF Security Server Command Language Reference*. The commands and the functions related to auditing are:

- **LISTDSD.** Lists the contents of data set profiles. If you have the AUDITOR attribute or the ROAUDIT attribute, you can list all profiles; if you have the group-AUDITOR attribute, you can list only those profiles within the scope of your group and its subgroups.
- **LFILE.** Lists the contents of SFS file profiles. If you have the AUDITOR attribute, you can list all profiles; if you have the group-AUDITOR attribute, you can list only those profiles within the scope of your group and its subgroups.
- **LDIRECT.** Lists the contents of SFS directory profiles. If you have the AUDITOR attribute, you can list all profiles; if you have the group-AUDITOR attribute, you can list only those profiles within the scope of your group and its subgroups.
- **LISTGRP.** Lists the contents of group profiles. While the output does not contain any information directly related to specific audit controls, it does include information about the group structure and each user's authority within the group. This information may be useful to you. If you have the AUDITOR attribute or the ROAUDIT attribute, you can list all group profiles; if you have the group-AUDITOR attribute, you can list only the profiles within the scope of your group and its subgroups.
- **LISTUSER.** Lists the contents of user profiles. If you have the AUDITOR attribute or the ROAUDIT attribute, you can list all user profiles; if you have the group-AUDITOR attribute, you can list only those profiles within the scope of your group and its subgroups.
- **RLIST.** Lists the contents of general resource profiles. If you have the AUDITOR attribute or the ROAUDIT attribute, you can list all resource profiles; if you have the group-AUDITOR attribute, you can list only those profiles within the scope of your group and its subgroups.

Example 1

To list the complete profile for SIVLE's A-disk, which has virtual address 191, enter the following:

```
RLIST  VMMDISK  SIVLE.191  ALL
```

Example 2

To list the complete profile for the SFS file REPORT SCRIPT in file pool FP2, directory DIR2 for user ID SIVLE, enter the following command:

```
LFILE  REPORT  SCRIPT  FP2:SIVLE.DIR2  ALL
```

Example 3

To list the complete profile for the SFS directory DIR2 in file pool FP2 for the user with the user ID SIVLE, enter the following command:

```
LDIRECT  FP2:SIVLE.DIR2  ALL
```

Auditing Events on z/VM

An installation can use RACF commands to turn auditing on and off for a set of events (called z/VM events), on a system-wide basis or for an individual user. z/VM events include CP commands, diagnose codes, certain events related to communication among virtual machines, and certain spool file activities. These various z/VM events belong to the VMXEVENT class on z/VM.

To create profiles that enable you to meet the auditing and access checking needs of your installation, do the following.

1. Determine the needed VMXEVENT profiles by examining the z/VM events that must be audited in a given situation. Depending on requirements, situations may vary. After reviewing the various situations, create profiles that reflect the events that must be audited. Bear in mind that these profiles serve a dual purpose:

   - They serve as a way to audit a z/VM event. Note that when you indicate that CP should call RACF to audit an event, RACF audits that event regardless of whether a corresponding profile exists. This enables your installation to meet auditing requirements without having to spend a lot of time creating profiles. It does not mean, however, that you should erase any existing profiles that contain auditing specifications.

     For example, you can turn on auditing for LINK in a VMXEVENT profile. You can then audit all LINK attempts without creating any VMMDISK profiles.
   - They can be used to instruct CP to call RACF to perform access checking on designated z/VM events. The VMXEVENT profile *is not* used to make the access decision. The access decision is based on the profile that protects the resource. For example, if CP calls RACF to authorize a LINK request to a minidisk, a profile that protects that minidisk must exist in the VMMDISK class, and RACF bases its authorization on that VMMDISK profile.

   Given this flexibility, you should plan these profiles carefully. Consider the following:

   - You can use one profile to define both z/VM auditing and access calls to RACF, or you can use one profile to indicate that CP should call RACF to audit certain events and another profile to indicate that CP should call RACF to perform access checking on certain events.
   - A user with the SPECIAL attribute can define profiles in the VMXEVENT class, but the SPECIAL user *can only* set the *control* options for z/VM events in that profile; the SPECIAL user cannot specify auditing options for z/VM events in that profile. If the SPECIAL user wants the profile to contain also z/VM events to be audited, the SPECIAL user must place the user with the AUDITOR attribute on the access list, with an access of ALTER. Alternatively, the SPECIAL user could transfer ownership of the profile to the AUDITOR user.

     A user with the AUDITOR attribute and class authority to the VMXEVENT class can define profiles in the VMXEVENT class, but that user *can only* set the *audit* options for z/VM events in that profile; that user cannot specify *control* options for z/VM events in that profile.

     To allow your installation to have the greatest flexibility and make the best use of the profiles that protect z/VM events, the user with the AUDITOR attribute should have class authority to the VMXEVENT class. This allows the user with the AUDITOR attribute to define profiles and change audit specifications at will.
   - All the auditing you want performed at any given time must be defined in a VMXEVENT profile. Similarly, all calls you want CP to make to RACF for access checking at a given time must be defined in a VMXEVENT profile. However, you can combine both sets of events in the same profile, if at a given time you want CP to call RACF to audit certain z/VM events and to perform access checking on certain z/VM events.

     To easily adapt to changes in auditing requirements, you may want to define several VMXEVENT profiles to use as your auditing environment changes.
2. To activate the VMXEVENT resource class, enter the SETROPTS command as follows:

   ```
   SETROPTS CLASSACT(VMXEVENT)
   ```

Note: You must have the RACF system SPECIAL attribute to enter the SETROPTS CLASSACT command.

System z/VM Event Profile

A system z/VM event profile is a resource profile defined in the VMXEVENT class. The options set in a system z/VM event profile determine the type of auditing and control that takes place for all of the users on the system. The rest of this section discusses how to use a system z/VM event profile to audit and not audit z/VM events. For information specific to controlling z/VM events, see *z/VM: RACF Security Server Security Administrator's Guide*. If an individual z/VM event profile is present for any specific user, it takes precedence over a system z/VM event profile.

When the SECLABEL class is active, the audit records contain the security label of the user issuing the event. Three exceptions are:

- APPCPWVL
- SPTAPE
- UTLPRINT

When the SECLABEL class is active, VMXEVENT audit records contain the security label of the target resource (or user, if the resource is not protected by a resource profile).

To audit resource security labels in which the resource is protected by a resource profile, such as minidisks and restricted segments, auditing should be enabled in the resource profile. To audit resource security labels in which the resource is *not* protected by a resource profile, auditing should be enabled for the event in the VMXEVENT profile. If the SECLABEL class is not active, no security labels appear in the VMXEVENT audit records.

Creating a System z/VM Event Profile

Use the RDEFINE command to create a system z/VM event profile. The commands to define two similar profiles look like this:

```
RDEFINE VMXEVENT EVENTS1
RDEFINE VMXEVENT EVENTS2
```

Note: When you issue the RLIST command for a VMXEVENT profile, the output shows the z/VM events that are audited if that profile is used to refresh the system.

Adding z/VM Events to a System z/VM Event Profile

Use the RALTER command to alter the profile to include a member list of z/VM events that are to be audited. For example, the following command specifies that, when profile EVENTS1 is in effect on the system, RACF audits the ATTACH and ACNT commands.

```
RALTER VMXEVENT EVENTS1 ADDMEM(ATTACH/AUDIT ACNT/AUDIT)
```

The first part of the member name (z/VM event that you want audited) must match **exactly** the "z/VM EVENT" shown in the output of the SETEVENT LIST command. See the sample output in Figure 3 on page 27.

You can issue the RALTER command as many times as you need to for one VMXEVENT profile, adding or deleting members as necessary.

Note:

1. You can combine creating and altering the profile by specifying the ADDMEM operand on the RDEFINE command.
2. If you use the RACF ISPF panels to update a VMXEVENT profile, you can select z/VM event names from a list on the panel.
3. The options set in this profile do not take effect until SETEVENT REFRESH is issued.
4. When you issue the RLIST command for a VMXEVENT profile, the output shows the members that have been added to the profile.

5. With CP exit support on z/VM, you can:
   - Dynamically add your own commands and diagnose codes to the CP nucleus
   - Audit these commands and diagnose codes using VMXEVENT profiles

Attention:
You must be careful with the characters you use in a command name. For example, the slash character (**/**) may interfere with the syntax of the RDEFINE or RALTER command you would use to define or alter your VMXEVENT profile. IBM recommends that you use *only* alphanumeric characters for any command name you want to audit using RACF.

Activating a System z/VM Event Profile

Use the SETEVENT command to specify which VMXEVENT profile you want active. The default of SETEVENT is no auditing of z/VM events. Depending on the auditing requirements of your environment at a given time, various profiles are appropriate to meet those requirements. For example, the following command specifies that profile EVENTS1 will be used to audit commands on the system. This also activates access checking set in the profile EVENTS1.

```
SETEVENT REFRESH EVENTS1
```

Note:

1. Once you activate a system z/VM event profile, it remains active until you change it.
2. The auditing of events using the SETEVENT command is in addition to the type of auditing you can invoke using the auditing keywords on the SETROPTS command.

Stopping the Auditing of a Specific z/VM Event in a System z/VM Event Profile

To stop auditing a specific z/VM event within a system z/VM event profile, do the following:

1. Identify the profile that was last used to set auditing on the system. You can compare the output from the SETEVENT LIST command (which shows the actual settings on the system) with the output from the RLIST command (which shows the settings that would be made from a VMXEVENT profile).

   For example, on z/VM, suppose SETEVENT LIST indicates that the SPOOL and TAG commands are to be audited. If the output of the command RLIST VMXEVENT EVENTS (Figure 2 on page 23) is the following, then the z/VM event profile EVENTS was most likely the last used to set auditing on the system.

```
CLASS      NAME
-----      ----
VMXEVENT    EVENTS

MEMBER CLASS NAME
------ ----- ----
VXMBR

OPTION  z/VM EVENT AUDIT AND/OR CONTROL MEMBERS
------  -----------------------------------
IN      DIAL
IN      MESSAGE.G
AUDIT   SPOOL
AUDIT   TAG

LEVEL  OWNER      UNIVERSAL ACCESS  YOUR ACCESS  WARNING
-----  --------   ----------------  -----------  -------
 00    IBMUSER         NONE              ALTER    NO

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

APPLICATION DATA
----------------
NONE

AUDITING
--------
FAILURES(READ)

GLOBALAUDIT
-----------
NONE

NOTIFY
------
NO USER TO BE NOTIFIED
```

Figure 2. Output from RLIST VMXEVENT EVENTS Command

2. Update the VMXEVENT profile using the RALTER command with the DELMEM operand.

   For example, the following command changes profile EVENTS so that TAG is not audited when profile EVENTS is in effect.

   ```
   RALTER VMXEVENT EVENTS DELMEM(TAG/AUDIT)
   ```

3. Use the SETEVENT REFRESH command to refresh the system with that profile.

   ```
   SETEVENT REFRESH EVENTS
   ```

   Note: Only users with the AUDITOR attribute can add or delete events that have been designated with the AUDIT option in the profile. In addition, only users with the AUDITOR attribute can issue the SETEVENT command to refresh the events they have chosen to audit.

Individual z/VM Event Profile

The main objective in using an individual z/VM event profile is to identify those users on the system who have unique circumstances in regard to auditing and access control, and to tailor selective profiles to monitor them in a specific way, which may result in either more or less monitoring for these users than the rest of the users on the system. Performance can be improved by the use of individually defined profiles tailored to individual users. The improvement results from a decrease in calls to the RACF service machine and in I/O to the SMF minidisk.

An individual z/VM event profile is a resource profile defined in the VMXEVENT class. The options set in an individual z/VM event profile determine the type of auditing and control that will take place for the user. If present, an individual z/VM event profile takes precedence over a system z/VM event profile in determining when CP calls RACF. The rest of the section discusses how to use an individual z/VM event profile to audit and not audit z/VM events. For information about controlling z/VM events, see *z/VM: RACF Security Server Security Administrator's Guide*.

Using Individual z/VM Event Profiles to Control Auditing

An installation may want to audit a diagnose instruction when a particular user enters it. In this instance, the installation creates an individual z/VM event profile that specifies auditing for that diagnose instruction. At the same time, assume that the options in the system z/VM event profile specify no auditing for that diagnose instruction. Using an individual z/VM event profile and system z/VM event profile in this way improves system performance, and at the same time provides the necessary auditing.

For example, the following command causes auditing to occur only when USER1 invokes DIAGNOSE X'08' provided auditing is not on for DIAGNOSE X'08' in the system z/VM event profile:

```
RDEFINE VMXEVENT USERSEL.USER1 ADDMEM(DIAG008/AUDIT)
```

The reverse situation can occur. The installation can define a system z/VM event profile to effect system-wide auditing for a particular diagnose instruction. However, assume the installation decides that a specific user does not need to be audited when issuing that diagnose instruction. In this case, the installation creates an individual z/VM event profile in which the user is not audited when issuing this diagnose instruction.

Creating an Individual z/VM Event Profile

Use the RDEFINE command to create an individual z/VM event profile. There can be only one individual z/VM event profile per user. Individual z/VM event profiles are distinguished from system z/VM event profiles by a high level qualifier called USERSEL. To identify the profile you are creating as an individual z/VM event profile, you must specify the high-level qualifier, followed by the user's user ID.

For example, if you wanted to create an individual z/VM event profile for a user with the user ID of FRANK, enter the following command:

```
RDEFINE VMXEVENT USERSEL.FRANK
```

Note: When you issue the RLIST command for a VMXEVENT profile, the output shows the z/VM events that are audited if that profile is used to refresh the system.

Adding z/VM Events to an Individual z/VM Event Profile

Use the RALTER command to alter the profile to include a member list of z/VM events that are to be audited for the user. For example, the following command specifies that when profile USERSEL.FRANK is in effect on the system, RACF audits each time user ID FRANK issues the ATTACH and the LINK commands.

```
RALTER VMXEVENT USERSEL.FRANK ADDMEM(ATTACH/AUDIT LINK/AUDIT)
```

The first part of the member name (z/VM event that you want audited) must match exactly the "z/VM EVENT" shown in the output of the SETEVENT LIST command. A sample of SETEVENT LIST output appears later in this chapter.

You can issue the RALTER command as many times as you need to for one VMXEVENT profile, adding or deleting members as necessary.

Note:

1. You can combine creating and altering the profile by specifying the ADDMEM operand on the RDEFINE command.
2. If you use the RACF ISPF panels to update a VMXEVENT profile, you can select z/VM events from a list on the panel.
3. The options set in this profile do not take effect until SETEVENT REFRESH USERSEL.FRANK is entered or until user ID FRANK logs on again, is autologged, or reconnects.
4. When you issue the RLIST command for a VMXEVENT profile, the output shows the members that have been added to the profile.
5. With CP exit support on z/VM, you can:

- Dynamically add your own commands and diagnose codes to the CP nucleus
- Audit these commands and diagnose codes using VMXEVENT profiles

Attention:
You must be careful with the characters you use in a command name. For example, the slash character (**/**) may interfere with the syntax of the RDEFINE or RALTER command you would use to define or alter your VMXEVENT profile. IBM recommends that you use *only* alphanumeric characters for any command name you want to audit using RACF.

Activating an Individual z/VM Event Profile

An individual z/VM event profile is activated or refreshed automatically whenever the user logs on, is autologged, or reconnects. You can also refresh the profile while the user is currently logged on by using the SETEVENT REFRESH command. For example, the following command resets the control and auditing options for user FRANK:

```
SETEVENT REFRESH USERSEL.FRANK
```

Note that the user FRANK must be logged on when the SETEVENT REFRESH is issued, or an error message will be displayed.

Stopping the Auditing of a Specific z/VM Event in an Individual z/VM Event Profile

To stop auditing a specific z/VM event within an individual z/VM event profile, do the following:

1. Update the VMXEVENT profile, using the RALTER command with the DELMEM operand.

   For example, the following command changes profile USERSEL.FRANK so that ATTACH is not audited when profile USERSEL.FRANK is in effect:

   ```
   RALTER VMXEVENT USERSEL.FRANK DELMEM(ATTACH/AUDIT)
   ```

2. Use the SETEVENT REFRESH command to refresh the system with that profile.

   ```
   SETEVENT REFRESH USERSEL.FRANK
   ```

   Note: Only users with the AUDITOR attribute can add or delete events that have been designated with the AUDIT option in the profile. In addition, only users with the AUDITOR attribute can issue the SETEVENT command to refresh the events they have chosen to audit.

Suspending an Individual z/VM Event Profile

Use the SETEVENT RESET command to return a user to the auditing set in a system z/VM event profile. For example, to discontinue individual auditing for user ID FRANK and have user ID FRANK audited through the system z/VM event profile in effect at the time, enter the following command:

```
SETEVENT RESET USERSEL.FRANK
```

Note:

1. The SETEVENT RESET command does not delete the individual z/VM event profile for user ID FRANK. Issuing the command simply means that you *temporarily suspend* the use of the individual z/VM event profile that has been established for user ID FRANK. The suspension will stay in effect until you issue a REFRESH for user ID FRANK's individual z/VM event profile or until user ID FRANK next logs on, or is autologged.
2. You use this same sequence to suspend the exempt status of a user, making that user subject to the system z/VM event profile in effect on the system.

Deleting an Individual z/VM Event Profile

Use the RDELETE and SETEVENT RESET commands to not merely suspend, but to *delete* an individual z/VM event profile. For example, to delete user ID FRANK's individual z/VM event profile and have user ID FRANK be subject to the system z/VM event profile that is in effect on the system, follow this sequence.

1. First, delete the user's individual z/VM event profile to ensure that the user's individual z/VM event profile won't be reactivated at logon. Enter the following command:

   ```
   RDELETE VMXEVENT USERSEL.FRANK
   ```

2. Second, issue the SETEVENT RESET command to deactivate the user's individual z/VM event profile. The high-level qualifier is required when issuing this command, even though the previous command has in fact removed the individual z/VM event profile.

   ```
   SETEVENT RESET USERSEL.FRANK
   ```

You use this same sequence to delete the exempt status of a user by removing the user's individual z/VM event profile, thus making that user subject to the system z/VM event profile.

Note: You can specify RDELETE without specifying SETEVENT RESET and thus allow the user to be under the options of the user's individual z/VM event profile until the user logs off. However, if the user simply disconnects, and does not logoff, the user continues to be audited through the individual z/VM event profile. The safer course of action, if you want to stop the use of an individual z/VM event profile, is to issue the RDELETE and SETEVENT RESET commands in sequence.

z/VM Events That Can Be Audited

You can use the SETEVENT LIST command to generate a list of z/VM events that can be audited. The SETEVENT LIST output shows "AUDITABLE z/VM EVENTS". Refer to Figure 3 on page 27 through Figure 10 on page 34.

```
PRE-LOGON COMMANDS

COMMAND              CONFIGURED IN
-------              -------------
DIAL                   YES
MESSAGE.ANY            YES
UNDIAL                 YES


CONTROLLABLE VM EVENTS

VM EVENT                     STATUS     VM EVENT                     STATUS
--------                     ------     --------                     ------
COUPLE.G                     CONTROL    FOR.C                        CONTROL
FOR.G                        CONTROL    LINK                         CONTROL
STORE.C                      CONTROL    TAG                          CONTROL
TRANSFER.D                   CONTROL    TRANSFER.G                   CONTROL
TRSOURCE                     CONTROL    DIAG088                      CONTROL
DIAG0A0                      CONTROL    DIAG0D4                      CONTROL
DIAG0E4                      CONTROL    DIAG280                      CONTROL
APPCPWVL                     CONTROL    MDISK                        CONTROL
RSTDSEG                      CONTROL    RDEVCTRL                     CONTROL


AUDITABLE VM EVENTS

VM EVENT                     STATUS     VM EVENT                     STATUS
--------                     ------     --------                     ------
ACNT                         NO_AUDIT   ACTIVATE                     NO_AUDIT
ADJUNCT                      NO_AUDIT   ADSTOP                       NO_AUDIT
ASSOCIATE                    NO_AUDIT   AT                           NO_AUDIT
ATTACH                       NO_AUDIT   ATTN                         NO_AUDIT
AUTOLOG.A                    NO_AUDIT   AUTOLOG.B                    NO_AUDIT
BACKSPACE                    NO_AUDIT   BEGIN                        NO_AUDIT
CHANGE.D                     NO_AUDIT   CHANGE.G                     NO_AUDIT
CLOSE                        NO_AUDIT   COMMANDS                     NO_AUDIT
COMMIT                       NO_AUDIT   CONCOPY                      NO_AUDIT
COUPLE.G                     NO_AUDIT   CPACCESS                     NO_AUDIT
CPCACHE                      NO_AUDIT   CPHX                         NO_AUDIT
CPLISTFILE                   NO_AUDIT   CPRELEASE                   NO_AUDIT
CPFORMAT                     NO_AUDIT   CPTRAP                      NO_AUDIT
CPTYPE                       NO_AUDIT   CPU                         NO_AUDIT
CPVLOAD                      NO_AUDIT   CPXLOAD                     NO_AUDIT
CPXUNLOAD                    NO_AUDIT   DEACTIVE                    NO_AUDIT
DEACTIVATE                   NO_AUDIT   DEDICATE                    NO_AUDIT
DEFINE.A                     NO_AUDIT   DEFINE.B                    NO_AUDIT
DEFINE.E                     NO_AUDIT   DEFINE.G                    NO_AUDIT
DEFSEG                       NO_AUDIT   DEFSYS                      NO_AUDIT
DELETE                       NO_AUDIT   DESTAGE                     NO_AUDIT
DETACH.B                     NO_AUDIT   DETACH.G                    NO_AUDIT
DIAL                         NO_AUDIT   DISABLE.A                   NO_AUDIT
DISABLE.B                    NO_AUDIT   DISABLE.F                   NO_AUDIT
DISASSOCIATE                 NO_AUDIT   DISCARD                     NO_AUDIT
DISCONNECT                   NO_AUDIT   DISPLAY.C                   NO_AUDIT
DISPLAY.E                    NO_AUDIT   DISPLAY.G                   NO_AUDIT
```

Figure 3. Sample Output from the SETEVENT LIST Command for z/VM (Part 1 of 8)

```
DRAIN.B                   NO_AUDIT   DRAIN.D                   NO_AUDIT
DUMP.C                    NO_AUDIT   DUMP.E                    NO_AUDIT
DUMP.G                    NO_AUDIT   DUPLEX                    NO_AUDIT
ECHO                      NO_AUDIT   ENABLE.A                  NO_AUDIT
ENABLE.B                  NO_AUDIT   ENABLE.F                  NO_AUDIT
EXTERNAL                  NO_AUDIT   FLASHCOPY                 NO_AUDIT
FLUSH                     NO_AUDIT   FOR.C                     NO_AUDIT
FOR.G                     NO_AUDIT   FORCE                     NO_AUDIT
FORWARD                   NO_AUDIT   FREE.B                    NO_AUDIT
FREE.D                    NO_AUDIT   GIVE                      NO_AUDIT
HALT                      NO_AUDIT   HOLD.B                    NO_AUDIT
HOLD.D                    NO_AUDIT   HYPERSWAP                 NO_AUDIT
INDICATE.B                NO_AUDIT   INDICATE.C                NO_AUDIT
INDICATE.E                NO_AUDIT   INDICATE.G                NO_AUDIT
IPL                       NO_AUDIT   LINK                      NO_AUDIT
LOADBUF                   NO_AUDIT   LOADVFCB                  NO_AUDIT
LOCATE.C                  NO_AUDIT   LOCATE.E                  NO_AUDIT
LOCATEVM                  NO_AUDIT   LOCK                      NO_AUDIT
LOGON                     NO_AUDIT   LOGOFF                    NO_AUDIT
MESSAGE.A                 NO_AUDIT   MESSAGE.B                 NO_AUDIT
MESSAGE.ANY               NO_AUDIT   MODIFY.A                  NO_AUDIT
MODIFY.B                  NO_AUDIT   MONITOR.A                 NO_AUDIT
MONITOR.E                 NO_AUDIT   MSGNOH                    NO_AUDIT
NOTREADY                  NO_AUDIT   ORDER.D                   NO_AUDIT
ORDER.G                   NO_AUDIT   PURGE.A                   NO_AUDIT
PURGE.B                   NO_AUDIT   PURGE.C                   NO_AUDIT
PURGE.D                   NO_AUDIT   PURGE.E                   NO_AUDIT
PURGE.G                   NO_AUDIT   READY                     NO_AUDIT
RECORDING.A               NO_AUDIT   RECORDING.B               NO_AUDIT
RECORDING.C               NO_AUDIT   RECORDING.E               NO_AUDIT
RECORDING.F               NO_AUDIT   REDEFINE                  NO_AUDIT
REFRESH                   NO_AUDIT   REPEAT                    NO_AUDIT
REQUEST                   NO_AUDIT   RESET.B                   NO_AUDIT
RESET.G                   NO_AUDIT   RESTART.A                 NO_AUDIT
RESTART.B                 NO_AUDIT   RESTART.G                 NO_AUDIT
RETAIN                    NO_AUDIT   REWIND                    NO_AUDIT
SAVESEG                   NO_AUDIT   SAVESYS                   NO_AUDIT
SCREEN                    NO_AUDIT   SEND.C                    NO_AUDIT
SEND.G                    NO_AUDIT   SHUTDOWN                 NO_AUDIT
SIGNAL.A                  NO_AUDIT   SIGNAL.C                  NO_AUDIT
SIGNAL.G                  NO_AUDIT   SILENTLY                  NO_AUDIT
SLEEP                     NO_AUDIT   SMSG                      NO_AUDIT
SNAPDUMP                  NO_AUDIT   SPACE                     NO_AUDIT
SPOOL                     NO_AUDIT   SPXTAPE.D                NO_AUDIT
SPXTAPE.E                 NO_AUDIT   SPXTAPE.G                NO_AUDIT
START.B                   NO_AUDIT   START.D                   NO_AUDIT
STOP                      NO_AUDIT   STORE.C                   NO_AUDIT
STORE.G                   NO_AUDIT   SYNCMDRS.A                NO_AUDIT
SYNCMDRS.B                NO_AUDIT   SYNCMDRS.F                NO_AUDIT
SYSTEM                    NO_AUDIT   TAG                       NO_AUDIT
TERMINAL                  NO_AUDIT   TRACE                     NO_AUDIT
TRANSFER.D                NO_AUDIT   TRANSFER.G                NO_AUDIT
TRSAVE.A                  NO_AUDIT   TRSAVE.C                  NO_AUDIT
```

Figure 4. Sample Output from the SETEVENT LIST Command for z/VM (Part 2 of 8)

```
TRSOURCE                    NO_AUDIT   UNCOUPLE                    NO_AUDIT
UNDEDICATE                  NO_AUDIT   UNDIAL                      NO_AUDIT
UNLOCK                      NO_AUDIT   VARY                        NO_AUDIT
VDELETE                     NO_AUDIT   VINPUT                      NO_AUDIT
VMDUMP                      NO_AUDIT   VMRELOCATE                  NO_AUDIT
WARNING.A                   NO_AUDIT   WARNING.B                   NO_AUDIT
WARNING.C                   NO_AUDIT   XAUTOLOG.A                  NO_AUDIT
XAUTOLOG.B                  NO_AUDIT   XAUTOLOG.G                  NO_AUDIT
XLINK.A                     NO_AUDIT   XLINK.B                     NO_AUDIT
XSPOOL.D                    NO_AUDIT   XSPOOL.G                    NO_AUDIT
QUERY.ABEND                 NO_AUDIT   QUERY.ACCOUNT               NO_AUDIT
QUERY.ADJUNCT               NO_AUDIT   QUERY.ALL                   NO_AUDIT
QUERY.ALLOC                 NO_AUDIT   QUERY.BYUSER.E              NO_AUDIT
QUERY.BYUSER.ANY            NO_AUDIT   QUERY.CACHE                 NO_AUDIT
QUERY.CACHEFW               NO_AUDIT   QUERY.CAPABILITY.A          NO_AUDIT
QUERY.CAPABILITY.B          NO_AUDIT   QUERY.CAPABILITY.C          NO_AUDIT
QUERY.CAPABILITY.E          NO_AUDIT   QUERY.CFLINKS.A             NO_AUDIT
QUERY.CFLINKS.B             NO_AUDIT   QUERY.CFLINKS.G             NO_AUDIT
QUERY.CHANNEL.A             NO_AUDIT   QUERY.CHANNEL.C             NO_AUDIT
QUERY.CHANNEL.E             NO_AUDIT   QUERY.CHPID                 NO_AUDIT
QUERY.CHPIDS.B              NO_AUDIT   QUERY.CHPIDS.E              NO_AUDIT
QUERY.CHPIDV                NO_AUDIT   QUERY.CMDLIMIT.A            NO_AUDIT
QUERY.CMDLIMIT.B            NO_AUDIT   QUERY.COLLECT               NO_AUDIT
QUERY.COMMANDS              NO_AUDIT   QUERY.CONCOPY               NO_AUDIT
QUERY.CONFIGMODE.B          NO_AUDIT   QUERY.CONFIGMODE.E          NO_AUDIT
QUERY.CONTROLLER            NO_AUDIT   QUERY.CONV                  NO_AUDIT
QUERY.CPASSIST.A            NO_AUDIT   QUERY.CPASSIST.C            NO_AUDIT
QUERY.CPASSIST.E            NO_AUDIT   QUERY.CPCHECKING.A          NO_AUDIT
QUERY.CPCHECKING.C          NO_AUDIT   QUERY.CPCHECKING.E          NO_AUDIT
QUERY.CPCMDS.A              NO_AUDIT   QUERY.CPCMDS.C              NO_AUDIT
QUERY.CPCMDS.E              NO_AUDIT   QUERY.CPDISKS               NO_AUDIT
QUERY.CPLANGUAGE            NO_AUDIT   QUERY.CPLANGLIST            NO_AUDIT
QUERY.CPLEVEL               NO_AUDIT   QUERY.CPLOAD.A              NO_AUDIT
QUERY.CPLOAD.B              NO_AUDIT   QUERY.CPLOAD.E              NO_AUDIT
QUERY.CPOWNED               NO_AUDIT   QUERY.CPTRACE.A             NO_AUDIT
QUERY.CPTRACE.C             NO_AUDIT   QUERY.CPTRACE.E             NO_AUDIT
QUERY.CPTRAP                NO_AUDIT   QUERY.CPUAFFINITY           NO_AUDIT
QUERY.CPUID                 NO_AUDIT   QUERY.CPXLOAD.A             NO_AUDIT
QUERY.CPXLOAD.C             NO_AUDIT   QUERY.CPXLOAD.E             NO_AUDIT
QUERY.CRYPTO.A              NO_AUDIT   QUERY.CRYPTO.B              NO_AUDIT
QUERY.CRYPTO.C              NO_AUDIT   QUERY.CRYPTO.E              NO_AUDIT
QUERY.CTCA                  NO_AUDIT   QUERY.CU                    NO_AUDIT
QUERY.DASD                  NO_AUDIT   QUERY.DASDFW                NO_AUDIT
QUERY.DATEFORMAT            NO_AUDIT   QUERY.DIAGNOSE.A            NO_AUDIT
QUERY.DIAGNOSE.C            NO_AUDIT   QUERY.DIAGNOSE.E            NO_AUDIT
QUERY.DUPLEX                NO_AUDIT   QUERY.DISPLAY               NO_AUDIT
QUERY.DUMP                  NO_AUDIT   QUERY.DUMPDEV               NO_AUDIT
QUERY.DYNAMIC_IO.B          NO_AUDIT   QUERY.DYNAMIC_IO.E          NO_AUDIT
QUERY.D8ONECMD.A            NO_AUDIT   QUERY.D8ONECMD.C            NO_AUDIT
QUERY.D8ONECMD.E            NO_AUDIT   QUERY.D8ONECMD.G            NO_AUDIT
QUERY.EDEVICE               NO_AUDIT   QUERY.EQID                  NO_AUDIT
QUERY.EXITS.A               NO_AUDIT   QUERY.EXITS.C               NO_AUDIT
QUERY.EXITS.E               NO_AUDIT   QUERY.FCP                   NO_AUDIT
QUERY.FENCES                NO_AUDIT   QUERY.FILES.D              NO_AUDIT
QUERY.FILES.G               NO_AUDIT   QUERY.FLASHCOPY             NO_AUDIT
QUERY.FRAMES.A              NO_AUDIT   QUERY.FRAMES.B              NO_AUDIT
QUERY.FRAMES.E              NO_AUDIT   QUERY.GATEWAY               NO_AUDIT
QUERY.GRAF                  NO_AUDIT   QUERY.HCD                   NO_AUDIT
```

Figure 5. Sample Output from the SETEVENT LIST Command for z/VM (Part 3 of 8)

```
QUERY.HOLD.B                NO_AUDIT   QUERY.HOLD.D                NO_AUDIT
QUERY.HOTIO                 NO_AUDIT   QUERY.HYPERSWAP             NO_AUDIT
QUERY.ICLNAME.A             NO_AUDIT   QUERY.ICLNAME.C             NO_AUDIT
QUERY.ICLNAME.E             NO_AUDIT   QUERY.IMG.A                 NO_AUDIT
QUERY.IMG.B                 NO_AUDIT   QUERY.IMG.C                 NO_AUDIT
QUERY.IMG.D                 NO_AUDIT   QUERY.IMG.E                 NO_AUDIT
QUERY.IOASSIST              NO_AUDIT   QUERY.IOPRIORITY.A          NO_AUDIT
QUERY.IOPRIORITY.E          NO_AUDIT   QUERY.IPLPARMS              NO_AUDIT
QUERY.ISFC                  NO_AUDIT   QUERY.ISLINK                NO_AUDIT
QUERY.IUCV.B                NO_AUDIT   QUERY.IUCV.G                NO_AUDIT
QUERY.JOURNAL.A             NO_AUDIT   QUERY.JOURNAL.E             NO_AUDIT
QUERY.KEYALIAS              NO_AUDIT   QUERY.LDEVS.B               NO_AUDIT
QUERY.LDEVS.G               NO_AUDIT   QUERY.LINES                 NO_AUDIT
QUERY.LINKS                 NO_AUDIT   QUERY.LKFAC                NO_AUDIT
QUERY.LKFACR                NO_AUDIT   QUERY.LOADDEV               NO_AUDIT
QUERY.LOGMSG.A              NO_AUDIT   QUERY.LOGMSG.B              NO_AUDIT
QUERY.LOGMSG.C              NO_AUDIT   QUERY.LOGMSG.D              NO_AUDIT
QUERY.LOGMSG.E              NO_AUDIT   QUERY.LOGMSG.F              NO_AUDIT
QUERY.LOGMSG.G              NO_AUDIT   QUERY.LAN.B                 NO_AUDIT
QUERY.LAN.G                 NO_AUDIT   QUERY.LPARS                 NO_AUDIT
QUERY.LSYSTEM               NO_AUDIT   QUERY.MAXLDEV               NO_AUDIT
QUERY.MAXSPOOL.D            NO_AUDIT   QUERY.MAXSPOOL.G            NO_AUDIT
QUERY.MAXUSERS              NO_AUDIT   QUERY.MDCACHE.B             NO_AUDIT
QUERY.MDCACHE.G             NO_AUDIT   QUERY.MDISK                 NO_AUDIT
QUERY.MEMASSIST.B           NO_AUDIT   QUERY.MEMASSIST.G           NO_AUDIT
QUERY.MITIME.A              NO_AUDIT   QUERY.MITIME.B              NO_AUDIT
QUERY.MONDATA               NO_AUDIT   QUERY.MONITOR.A             NO_AUDIT
QUERY.MONITOR.E             NO_AUDIT   QUERY.MSS                   NO_AUDIT
QUERY.NAMES.A               NO_AUDIT   QUERY.NAMES.B               NO_AUDIT
QUERY.NAMES.C               NO_AUDIT   QUERY.NAMES.D               NO_AUDIT
QUERY.NAMES.E               NO_AUDIT   QUERY.NAMES.F               NO_AUDIT
QUERY.NAMES.G               NO_AUDIT   QUERY.NEW_DEVICES           NO_AUDIT
QUERY.NIC                   NO_AUDIT   QUERY.NLS                   NO_AUDIT
QUERY.NSS                   NO_AUDIT   QUERY.NVS                   NO_AUDIT
QUERY.OBSERVER.A            NO_AUDIT   QUERY.OBSERVER.B            NO_AUDIT
QUERY.OBSERVER.C            NO_AUDIT   QUERY.OBSERVER.G            NO_AUDIT
QUERY.OSA                   NO_AUDIT   QUERY.PAGING.A              NO_AUDIT
QUERY.PAGING.C              NO_AUDIT   QUERY.PAGING.E              NO_AUDIT
QUERY.PASSWORD              NO_AUDIT   QUERY.PATHS.B               NO_AUDIT
QUERY.PATHS.E               NO_AUDIT   QUERY.PAV                   NO_AUDIT
QUERY.PENDING               NO_AUDIT   QUERY.PINNED                NO_AUDIT
QUERY.PF                    NO_AUDIT   QUERY.PORT                  NO_AUDIT
QUERY.PRINTER.D             NO_AUDIT   QUERY.PRINTER.G             NO_AUDIT
QUERY.PRIORITY.A            NO_AUDIT   QUERY.PRIORITY.B            NO_AUDIT
QUERY.PRIORITY.E            NO_AUDIT   QUERY.PRIORITY.F            NO_AUDIT
QUERY.PRIVCLASS.C           NO_AUDIT   QUERY.PRIVCLASS.E           NO_AUDIT
QUERY.PRIVCLASS.ANY         NO_AUDIT   QUERY.PROCESSORS.A          NO_AUDIT
QUERY.PROCESSORS.B          NO_AUDIT   QUERY.PROCESSORS.C          NO_AUDIT
QUERY.PROCESSORS.E          NO_AUDIT   QUERY.PRODUCT.C             NO_AUDIT
QUERY.PRODUCT.E             NO_AUDIT   QUERY.PROMPT                NO_AUDIT
QUERY.PSWTRANS              NO_AUDIT   QUERY.PUNCH.D               NO_AUDIT
QUERY.PUNCH.G               NO_AUDIT   QUERY.PVMSG                 NO_AUDIT
QUERY.QIOASSIST.B           NO_AUDIT   QUERY.QIOASSIST.G           NO_AUDIT
QUERY.QDROP.A               NO_AUDIT   QUERY.QDROP.B               NO_AUDIT
QUERY.QDROP.E               NO_AUDIT   QUERY.QDROP.F               NO_AUDIT
QUERY.QUICKDSP.A            NO_AUDIT   QUERY.QUICKDSP.E            NO_AUDIT
QUERY.READER.D              NO_AUDIT   QUERY.READER.G              NO_AUDIT
```

Figure 6. Sample Output from the SETEVENT LIST Command for z/VM (Part 4 of 8)

```
QUERY.RECORDING.A           NO_AUDIT   QUERY.RECORDING.B           NO_AUDIT
QUERY.RECORDING.C           NO_AUDIT   QUERY.RECORDING.E           NO_AUDIT
QUERY.RECORDING.F           NO_AUDIT   QUERY.REORDER.B             NO_AUDIT
QUERY.REORDER.E             NO_AUDIT   QUERY.RELODOMAIN.A          NO_AUDIT
QUERY.RELODOMAIN.B          NO_AUDIT   QUERY.RELODOMAIN.C          NO_AUDIT
QUERY.RELODOMAIN.E          NO_AUDIT   QUERY.RESERVED.A            NO_AUDIT
QUERY.RESERVED.E            NO_AUDIT   QUERY.RESOURCE              NO_AUDIT
QUERY.RETRIEVE              NO_AUDIT   QUERY.RSAW                  NO_AUDIT
QUERY.SASSIST.A             NO_AUDIT   QUERY.SASSIST.C             NO_AUDIT
QUERY.SASSIST.E             NO_AUDIT   QUERY.SCMBKS.B              NO_AUDIT
QUERY.SCMBKS.E              NO_AUDIT   QUERY.SCMEASURE.B           NO_AUDIT
QUERY.SCMEASURE.E           NO_AUDIT   QUERY.SCREEN                NO_AUDIT
QUERY.SDF.A                 NO_AUDIT   QUERY.SDF.B                 NO_AUDIT
QUERY.SDF.C                 NO_AUDIT   QUERY.SDF.D                 NO_AUDIT
QUERY.SDF.E                 NO_AUDIT   QUERY.SDF.G                 NO_AUDIT
QUERY.SECUSER.A             NO_AUDIT   QUERY.SECUSER.B             NO_AUDIT
QUERY.SECUSER.C             NO_AUDIT   QUERY.SECUSER.G             NO_AUDIT
QUERY.SET                   NO_AUDIT   QUERY.SHARE.A               NO_AUDIT
QUERY.SHARE.E               NO_AUDIT   QUERY.SHUTDOWNTIME.A        NO_AUDIT
QUERY.SHUTDOWNTIME.C        NO_AUDIT   QUERY.SIGNAL                NO_AUDIT
QUERY.SIGNALS               NO_AUDIT   QUERY.SPACES.E              NO_AUDIT
QUERY.SPACES.G              NO_AUDIT   QUERY.SPMODE.A              NO_AUDIT
QUERY.SPMODE.C              NO_AUDIT   QUERY.SPMODE.E              NO_AUDIT
QUERY.SRM.A                 NO_AUDIT   QUERY.SRM.E                 NO_AUDIT
QUERY.SSI.B                 NO_AUDIT   QUERY.SSI.E                 NO_AUDIT
QUERY.STGEXEMPT.A           NO_AUDIT   QUERY.STGEXEMPT.B           NO_AUDIT
QUERY.STGEXEMPT.C           NO_AUDIT   QUERY.STGEXEMPT.E           NO_AUDIT
QUERY.STGEXEMPT.G           NO_AUDIT   QUERY.STGLIMIT.A            NO_AUDIT
QUERY.STGLIMIT.B            NO_AUDIT   QUERY.STGLIMIT.C            NO_AUDIT
QUERY.STGLIMIT.E            NO_AUDIT   QUERY.STORAGE.A             NO_AUDIT
QUERY.STORAGE.B             NO_AUDIT   QUERY.STORAGE.E             NO_AUDIT
QUERY.STP                   NO_AUDIT   QUERY.SUBSTITUTE            NO_AUDIT
QUERY.SWITCHES              NO_AUDIT   QUERY.SXSPAGES.A            NO_AUDIT
QUERY.SXSPAGES.B            NO_AUDIT   QUERY.SXSPAGES.E            NO_AUDIT
QUERY.SXSSTORAGE.A          NO_AUDIT   QUERY.SXSSTORAGE.B          NO_AUDIT
QUERY.SXSSTORAGE.E          NO_AUDIT   QUERY.SYSASCII              NO_AUDIT
QUERY.SYSOPER               NO_AUDIT   QUERY.SYSTEM                NO_AUDIT
QUERY.S370E.A               NO_AUDIT   QUERY.S370E.C               NO_AUDIT
QUERY.S370E.E               NO_AUDIT   QUERY.TAG                   NO_AUDIT
QUERY.TAPES                 NO_AUDIT   QUERY.TDISK                 NO_AUDIT
QUERY.TDISKCLR              NO_AUDIT   QUERY.TERMINAL              NO_AUDIT
QUERY.THROTTLE.B            NO_AUDIT   QUERY.THROTTLE.E            NO_AUDIT
QUERY.TIME                  NO_AUDIT   QUERY.TIMEZONES             NO_AUDIT
QUERY.TOKEN                 NO_AUDIT   QUERY.TRACE                 NO_AUDIT
QUERY.TRACEFRAMES.A         NO_AUDIT   QUERY.TRACEFRAMES.B         NO_AUDIT
QUERY.TRACEFRAMES.C         NO_AUDIT   QUERY.TRACEFRAMES.E         NO_AUDIT
QUERY.TRFILES.A             NO_AUDIT   QUERY.TRFILES.C             NO_AUDIT
QUERY.TRFILES.D             NO_AUDIT   QUERY.TRFILES.E             NO_AUDIT
QUERY.TRFILES.G             NO_AUDIT   QUERY.TRSAVE.A              NO_AUDIT
QUERY.TRSAVE.C              NO_AUDIT   QUERY.TRSAVE.E              NO_AUDIT
QUERY.TRSAVE.G              NO_AUDIT   QUERY.TRSOURCE.A            NO_AUDIT
QUERY.TRSOURCE.C            NO_AUDIT   QUERY.TRSOURCE.E            NO_AUDIT
QUERY.TRSOURCE.G            NO_AUDIT   QUERY.UCR.A                 NO_AUDIT
QUERY.UCR.B                 NO_AUDIT   QUERY.UCR.C                 NO_AUDIT
QUERY.UNDERSCORE            NO_AUDIT   QUERY.UNRESOLVED.A          NO_AUDIT
QUERY.UNRESOLVED.C          NO_AUDIT   QUERY.UNRESOLVED.E          NO_AUDIT
QUERY.UR                    NO_AUDIT   QUERY.USERID                NO_AUDIT
QUERY.USERS                 NO_AUDIT   QUERY.VCONFIG              NO_AUDIT
QUERY.VDISK                 NO_AUDIT   QUERY.VMDUMP               NO_AUDIT
QUERY.VMLAN                 NO_AUDIT   QUERY.VMSAVE.A             NO_AUDIT
QUERY.VMSAVE.C              NO_AUDIT   QUERY.VMSAVE.E             NO_AUDIT
QUERY.VMRELOCATE.A          NO_AUDIT   QUERY.VMRELOCATE.B         NO_AUDIT
QUERY.VMRELOCATE.C          NO_AUDIT   QUERY.VMRELOCATE.E         NO_AUDIT
QUERY.VMSG                  NO_AUDIT   QUERY.VRFREE               NO_AUDIT
```

Figure 7. Sample Output from the SETEVENT LIST Command for z/VM (Part 5 of 8)

```
QUERY.VSWITCH.B              NO_AUDIT   QUERY.VSWITCH.G              NO_AUDIT
QUERY.VTOD.A                 NO_AUDIT   QUERY.VTOD.B                 NO_AUDIT
QUERY.VTOD.G                 NO_AUDIT   QUERY.VR                     NO_AUDIT
QUERY.WRKALLEG               NO_AUDIT   QUERY.XSTORAGE.B             NO_AUDIT
QUERY.XSTORAGE.E             NO_AUDIT   QUERY.V.ALL                  NO_AUDIT
QUERY.V.CHPID                NO_AUDIT   QUERY.V.CONSOLE              NO_AUDIT
QUERY.V.CPUS                 NO_AUDIT   QUERY.V.CRYPTO               NO_AUDIT
QUERY.V.CTCA                 NO_AUDIT   QUERY.V.DASD                 NO_AUDIT
QUERY.V.DUPLEX               NO_AUDIT   QUERY.V.FCP                  NO_AUDIT
QUERY.V.FLASHCOPY            NO_AUDIT   QUERY.V.GRAF                 NO_AUDIT
QUERY.V.LINES                NO_AUDIT   QUERY.V.MSGDEVICES           NO_AUDIT
QUERY.V.MSGPROC              NO_AUDIT   QUERY.V.NIC                  NO_AUDIT
QUERY.V.OSA                  NO_AUDIT   QUERY.V.PAV                  NO_AUDIT
QUERY.V.PRINTER              NO_AUDIT   QUERY.V.PUNCH                NO_AUDIT
QUERY.V.READER               NO_AUDIT   QUERY.V.STORAGE              NO_AUDIT
QUERY.V.SWITCHES             NO_AUDIT   QUERY.V.SYSASCII             NO_AUDIT
QUERY.V.TAPES                NO_AUDIT   QUERY.V.UR                   NO_AUDIT
QUERY.V.XSTORAGE             NO_AUDIT   QUERY.VIRTUAL.B              NO_AUDIT
QUERY.VIRTUAL.G              NO_AUDIT   SET.ABEND                    NO_AUDIT
SET.ACCOUNT                  NO_AUDIT   SET.ACNT                     NO_AUDIT
SET.ADJUNCTS                 NO_AUDIT   SET.AFFINITY                 NO_AUDIT
SET.ASSIST                   NO_AUDIT   SET.AUTOPOLL                 NO_AUDIT
SET.CACHE                    NO_AUDIT   SET.CACHEFW                  NO_AUDIT
SET.CCWTRAN                  NO_AUDIT   SET.CFLINK.A                 NO_AUDIT
SET.CFLINK.B                 NO_AUDIT   SET.CFLINK.G                 NO_AUDIT
SET.CMDLIMIT                 NO_AUDIT   SET.CONCEAL                  NO_AUDIT
SET.CONFIGMODE               NO_AUDIT   SET.CPASSIST                 NO_AUDIT
SET.CPCHECKING.A             NO_AUDIT   SET.CPCHECKING.C             NO_AUDIT
SET.CPCONIO                  NO_AUDIT   SET.CPLANGUAGE.B             NO_AUDIT
SET.CPLANGUAGE.G             NO_AUDIT   SET.CPTRACE.A                NO_AUDIT
SET.CPTRACE.C                NO_AUDIT   SET.CPUAFFINITY              NO_AUDIT
SET.CU                       NO_AUDIT   SET.CPUID                    NO_AUDIT
SET.DASDFW                   NO_AUDIT   SET.DATEFORMAT.B             NO_AUDIT
SET.DATEFORMAT.G             NO_AUDIT   SET.DEVICES                  NO_AUDIT
SET.DUMP                     NO_AUDIT   SET.DUMPDEV                  NO_AUDIT
SET.DYNAMIC_IO               NO_AUDIT   SET.D8ONECMD.A               NO_AUDIT
SET.D8ONECMD.G               NO_AUDIT   SET.ECMODE                   NO_AUDIT
SET.EDEVICE                  NO_AUDIT   SET.EMSG                     NO_AUDIT
SET.FAVORED                  NO_AUDIT   SET.HOTIO                    NO_AUDIT
SET.IMSG                     NO_AUDIT   SET.IOASSIST.B               NO_AUDIT
SET.IOASSIST.G               NO_AUDIT   SET.IOCDS_ACTIVE             NO_AUDIT
SET.IOPRIORITY               NO_AUDIT   SET.IPLPARMS                 NO_AUDIT
SET.ISAM                     NO_AUDIT   SET.JOURNAL                  NO_AUDIT
SET.KEYALIAS                 NO_AUDIT   SET.LAN.B                    NO_AUDIT
SET.LAN.G                    NO_AUDIT   SET.LINEDIT                  NO_AUDIT
SET.LKFAC                    NO_AUDIT   SET.LKFACR                   NO_AUDIT
SET.LOADDEV                  NO_AUDIT   SET.LOGMSG                   NO_AUDIT
SET.LSYSTEM                  NO_AUDIT   SET.MACHINE                  NO_AUDIT
SET.MAXLDEV                  NO_AUDIT   SET.MAXUSERS                 NO_AUDIT
SET.MDCACHE.B                NO_AUDIT   SET.MDCACHE.G                NO_AUDIT
SET.MEMASSIST.B              NO_AUDIT   SET.MEMASSIST.G              NO_AUDIT
SET.MSG                      NO_AUDIT   SET.MSGFACIL                 NO_AUDIT
SET.MIH                      NO_AUDIT   SET.MINWS                    NO_AUDIT
SET.MITIME.A                 NO_AUDIT   SET.MITIME.B                 NO_AUDIT
SET.MODE.A                   NO_AUDIT   SET.MODE.F                   NO_AUDIT
SET.MONDATA                  NO_AUDIT   SET.NEW_DEVICES              NO_AUDIT
SET.NIC.B                    NO_AUDIT   SET.NIC.G                    NO_AUDIT
SET.NOPDATA                  NO_AUDIT   SET.NOTRANS                  NO_AUDIT
```

Figure 8. Sample Output from the SETEVENT LIST Command for z/VM (Part 6 of 8)

```
SET.NVS                     NO_AUDIT   SET.OBSERVER.A              NO_AUDIT
SET.OBSERVER.C              NO_AUDIT   SET.OBSERVER.G              NO_AUDIT
SET.PAGEX                   NO_AUDIT   SET.PAGING                  NO_AUDIT
SET.PASSWORD                NO_AUDIT   SET.PF                      NO_AUDIT
SET.PORT                    NO_AUDIT   SET.PRIORITY.A              NO_AUDIT
SET.PRIORITY.B              NO_AUDIT   SET.PRIORITY.E              NO_AUDIT
SET.PRIORITY.F              NO_AUDIT   SET.PRIVCLASS.C             NO_AUDIT
SET.PRIVCLASS.ANY           NO_AUDIT   SET.PRODUCT.C               NO_AUDIT
SET.PRODUCT.E               NO_AUDIT   SET.PROMPT                  NO_AUDIT
SET.PSWTRANS                NO_AUDIT   SET.QIOASSIST.B             NO_AUDIT
SET.QIOASSIST.G             NO_AUDIT   SET.QUICKDSP                NO_AUDIT
SET.QDROP.A                 NO_AUDIT   SET.QDROP.B                 NO_AUDIT
SET.QDROP.E                 NO_AUDIT   SET.QDROP.F                 NO_AUDIT
SET.RECORD                  NO_AUDIT   SET.RDEVICE                 NO_AUDIT
SET.REORDER                 NO_AUDIT   SET.RESERVED                NO_AUDIT
SET.RETRIEVE.C              NO_AUDIT   SET.RETRIEVE.E              NO_AUDIT
SET.RETRIEVE.G              NO_AUDIT   SET.RUN                     NO_AUDIT
SET.SASSIST                 NO_AUDIT   SET.SCMEASURE.B             NO_AUDIT
SET.SCMEASURE.E             NO_AUDIT   SET.SECUSER.A               NO_AUDIT
SET.SECUSER.C               NO_AUDIT   SET.SECUSER.G               NO_AUDIT
SET.SHARE                   NO_AUDIT   SET.SHARED                  NO_AUDIT
SET.SHUTSIGNAL              NO_AUDIT   SET.SHUTDOWNTIME.A          NO_AUDIT
SET.SHUTDOWNTIME.C          NO_AUDIT   SET.SIGNAL.A                NO_AUDIT
SET.SIGNAL.C                NO_AUDIT   SET.SMSG                    NO_AUDIT
SET.SRM                     NO_AUDIT   SET.SSI                     NO_AUDIT
SET.STBYPASS                NO_AUDIT   SET.STGEXEMPT.A             NO_AUDIT
SET.STGEXEMPT.B             NO_AUDIT   SET.STGEXEMPT.C             NO_AUDIT
SET.STGLIMIT.A              NO_AUDIT   SET.STGLIMIT.B              NO_AUDIT
SET.STGLIMIT.C              NO_AUDIT   SET.STMULTI                 NO_AUDIT
SET.STORAGE                 NO_AUDIT   SET.SVCACCL                 NO_AUDIT
SET.SVC76                   NO_AUDIT   SET.SYSOPER                 NO_AUDIT
SET.S370E.A                 NO_AUDIT   SET.S370E.G                 NO_AUDIT
SET.TAPE                    NO_AUDIT   SET.THROTTLE                NO_AUDIT
SET.TIMEBOMB                NO_AUDIT   SET.TIMER                   NO_AUDIT
SET.TIMEZONE                NO_AUDIT   SET.TOKEN.B                 NO_AUDIT
SET.TOKEN.E                 NO_AUDIT   SET.TRACEFRAMES             NO_AUDIT
SET.UNDERSCORE              NO_AUDIT   SET.VCONFIG                 NO_AUDIT
SET.VDISK                   NO_AUDIT   SET.VMCONIO                 NO_AUDIT
SET.VMLAN                   NO_AUDIT   SET.VMRELOCATE              NO_AUDIT
SET.VMSAVE.A                NO_AUDIT   SET.VMSAVE.G                NO_AUDIT
SET.VSWITCH                 NO_AUDIT   SET.VTOD.A                  NO_AUDIT
SET.VTOD.B                  NO_AUDIT   SET.VTOD.G                  NO_AUDIT
SET.WNG                     NO_AUDIT   SET.WRKALLEG                NO_AUDIT
SET.370ACCOM                NO_AUDIT   SET.370E                    NO_AUDIT
DIAG000                     NO_AUDIT   DIAG004                     NO_AUDIT
DIAG008                     NO_AUDIT   DIAG00C                     NO_AUDIT
DIAG010                     NO_AUDIT   DIAG014                     NO_AUDIT
DIAG018                     NO_AUDIT   DIAG020                     NO_AUDIT
DIAG024                     NO_AUDIT   DIAG028                     NO_AUDIT
DIAG034                     NO_AUDIT   DIAG03C                     NO_AUDIT
DIAG040                     NO_AUDIT   DIAG044                     NO_AUDIT
DIAG048                     NO_AUDIT   DIAG04C                     NO_AUDIT
DIAG054                     NO_AUDIT   DIAG058                     NO_AUDIT
DIAG05C                     NO_AUDIT   DIAG060                     NO_AUDIT
DIAG064                     NO_AUDIT   DIAG068                     NO_AUDIT
DIAG070                     NO_AUDIT   DIAG074                     NO_AUDIT
DIAG07C                     NO_AUDIT   DIAG084                     NO_AUDIT
DIAG088                     NO_AUDIT   DIAG08C                     NO_AUDIT
DIAG090                     NO_AUDIT   DIAG094                     NO_AUDIT
DIAG098                     NO_AUDIT   DIAG09C                     NO_AUDIT
DIAG0A0                     NO_AUDIT   DIAG0A4                     NO_AUDIT
DIAG0A8                     NO_AUDIT   DIAG0B0                     NO_AUDIT
DIAG0B4                     NO_AUDIT   DIAG0B8                     NO_AUDIT
```

Figure 9. Sample Output from the SETEVENT LIST Command for z/VM (Part 7 of 8)

```
DIAG0BC                      NO_AUDIT   DIAG0C4                      NO_AUDIT
DIAG0C8                      NO_AUDIT   DIAG0CC                      NO_AUDIT
DIAG0D0                      NO_AUDIT   DIAG0D4                      NO_AUDIT
DIAG0D8                      NO_AUDIT   DIAG0DC                      NO_AUDIT
DIAG0E0                      NO_AUDIT   DIAG0E4                      NO_AUDIT
DIAG0EC                      NO_AUDIT   DIAG0F0                      NO_AUDIT
DIAG0F8                      NO_AUDIT   DIAG204                      NO_AUDIT
DIAG210                      NO_AUDIT   DIAG214                      NO_AUDIT
DIAG218                      NO_AUDIT   DIAG220                      NO_AUDIT
DIAG224                      NO_AUDIT   DIAG238                      NO_AUDIT
DIAG23C                      NO_AUDIT   DIAG240                      NO_AUDIT
DIAG244                      NO_AUDIT   DIAG248                      NO_AUDIT
DIAG250                      NO_AUDIT   DIAG254                      NO_AUDIT
DIAG258                      NO_AUDIT   DIAG25C                      NO_AUDIT
DIAG260                      NO_AUDIT   DIAG264                      NO_AUDIT
DIAG268                      NO_AUDIT   DIAG26C                      NO_AUDIT
DIAG270                      NO_AUDIT   DIAG274                      NO_AUDIT
DIAG278                      NO_AUDIT   DIAG27C                      NO_AUDIT
DIAG280                      NO_AUDIT   DIAG288                      NO_AUDIT
DIAG290                      NO_AUDIT   DIAG29C                      NO_AUDIT
DIAG2A0                      NO_AUDIT   DIAG2A4                      NO_AUDIT
DIAG2A8                      NO_AUDIT   DIAG2AC                      NO_AUDIT
DIAG2C0                      NO_AUDIT   DIAG2C4                      NO_AUDIT
DIAG2CC                      NO_AUDIT   DIAG2E0                      NO_AUDIT
DIAG2FC                      NO_AUDIT   DIAG308                      NO_AUDIT
IUCVCON                      NO_AUDIT   IUCVSEV                      NO_AUDIT
APPCCON                      NO_AUDIT   APPCPWVL                     NO_AUDIT
APPCSEV                      NO_AUDIT   SPF_CREATE                   NO_AUDIT
SPF_DELETE                   NO_AUDIT   SPF_OPEN                     NO_AUDIT
SDF_CREATE                   NO_AUDIT   SDF_DELETE                   NO_AUDIT
SDF_OPEN                     NO_AUDIT   UTLPRINT                     NO_AUDIT
MDISK                        NO_AUDIT   MAINTCCW                     NO_AUDIT
RSTDSEG                      NO_AUDIT   SNIFFER_MODE                NO_AUDIT
DIRECTRY_CMD                 NO_AUDIT   SCIF                         NO_AUDIT
RDEVCTRL                     NO_AUDIT   DEFINE.MDISK                 NO_AUDIT
RPISET126I SETEVENT COMPLETED SUCCESSFULLY.
```

Figure 10. Sample Output from the SETEVENT LIST Command for z/VM (Part 8 of 8)

In the SETEVENT LIST output, "VM EVENT" indicates the name of the z/VM event as RACF recognizes it. "STATUS" indicates one of the following:

- NO_AUDIT indicates that the event is not currently being audited on your system.
- AUDIT means that the event is being audited.

Attention:

Auditing can degrade system performance. In particular, auditing the following z/VM events can have a significant effect on system performance:

DIAGNOSE X'08'
DIAGNOSE X'10'
DIAGNOSE X'0C'
DIAGNOSE X'14'
DIAGNOSE X'18'
DIAGNOSE X'24'
DIAGNOSE X'58'
DIAGNOSE X'60'
DIAGNOSE X'64'
DIAGNOSE X'68'
DIAGNOSE X'7C'
DIAGNOSE X'98'
DIAGNOSE X'A4'
DIAGNOSE X'A8'
DIAGNOSE X'214'

Auditing other z/VM events that are commonly used, such as spool and tag checking and spool file opens and deletes, also can have a significant effect on system performance.

Note: RACF for z/VM always generates an SMF record for LOGON, AUTOLOG, and XAUTOLOG. RACF can record additional logging information if you specify LOGON, AUTOLOG, or XAUTOLOG with the audit option in the VMXEVENT profile with which you are refreshing.

Auditing Commands Issued from the CP Directory

The COMMAND directory control statement is an optional statement used to specify a CP command to be executed after the virtual machine is logged on. The command is executed as if the virtual machine is authorized for all privilege classes.

Use the DIRECTRY_CMD system event in your VMXEVENT profile to control auditing of all commands issued from the CP directory. Each command is audited in an SMF type 80 record in the VMXEVENT class using the group 4 mapping for general commands documented in *z/VM: RACF Security Server Macros and Interfaces*. Note that the use of the DIRECTRY_CMD event does not affect the authorization and auditing which may occur as a result of processing other CP directory options (for example, LINKs to minidisks) during LOGON.

Auditing CP Commands with the “TO” Option

You can audit all occurrences of a spool file being transferred by turning on audit for TRANSFER.D or TRANSFER.G. This covers files transferred as a result of the TRANSFER command or the CHANGE TO command. Spool files created as a result of CLOSE TO, SPOOL TO, SPOOL FOR, TRSAVE TO, and VMDUMP TO can be audited by turning on audit for SPF_CREATE.

Auditing CP Commands with the “ALL” Option

An audit record can be created for all spool files changed as a result of the CHANGE ALL command by turning on audit for CHANGE.D or CHANGE.G. Likewise, an audit record can be created for all spool files deleted as a result of the PURGE ALL command by turning on audit for SPF_DELETE.

Auditing the CP CHANGE Command with the SECLABEL Option

When the CHANGE command is issued with the SECLABEL option, the audit record indicates the spool file being changed, as well as the old and new SECLABEL of the spool file.

Auditing Restricted Segments

If auditing is turned on for RSTDSEG in the VMXEVENT profile, an audit record is created whenever a restricted segment is loaded.

Auditing Mandatory Access Checks

Mandatory access control (MAC) is a method of restricting access to resources based on the sensitivity of the information that the resource contains and the authorization of the user to access information with that level of sensitivity. The security administrator defines the sensitivity of the resource by means of a label. For more information, see *z/VM: RACF Security Server Security Administrator's Guide* and the definition for mandatory access control in the glossary.

Auditing Two Jobs with the Same User ID

When work is being done simultaneously by a user ID and by a batch machine operating on behalf of that user ID, the audit record must distinguish between the work done by the batch machine and the work done by the user ID. To do this, RACF includes the alternate user ID in all records created for the batch machine, for example:

1. BATCH1 is doing work on behalf of USERA.
2. BATCH1 issues:

   ```
   LINK WORKDISK 191 192 RR
   ```

   on behalf of USERA.
3. USERA issues:

   ```
   STORE H20000 FFFF
   ```

   on his own behalf.
4. The LINK audit record will contain both BATCH1 and USERA.
5. The STORE.C audit record will contain USERA.

All audit records created for a user ID that is doing work on behalf of another user ID will contain both user IDs.

Auditing for DEFINE MDISK

You can use RACF to audit definitions of z/VM minidisks using profile DEFINE.MDISK in the VMCMD resource class. The following event can be audited:

DEFINE MDISK Command
A user's attempt to dynamically define a minidisk on these media types:

- A system volume
- The DASD volume that is attached to the system

DEFINE.MDISK event
A user defining a minidisk.

DEFINE.MDISK can generate audit events that are created when the user issues a DEFINE MDISK command. The audit records for DEFINE MDISK contain the effective access right for the resource profile DEFINE.MDISK in class VMCMD, if any exists. Access intent UPDATE is always assumed, which is the minimum effective access right needed for success. An audit record can be created that contains the DEFINE MDISK command parameters by turning on audit for DEFINE.A.

For example, assume that RACF has been set up for access control and auditing of user SYSOP1 (a CP class A user):

```
RDEFINE VMCMD DEFINE.MDISK AUDIT(ALL,(READ)) UACC(NONE)
SETROPTS REFRESH RACLIST(VMCMD)
```

SYSOP1 executes the CP command:

```
DEFINE MDISK 200 100 100 VOL001
```

In this example, audit records may be written as demonstrated in the condensed XML excerpts for both variations of RACF permits:

Variation 1

```
PERMIT DEFINE.MDISK CLASS(VMCMD) ID(SYSOP1) ACCESS(READ)
```

or

Variation 2

```
PERMIT DEFINE.MDISK CLASS(VMCMD) ID(SYSOP1) ACCESS(UPDATE)
```

Note: XML can be generated by RACF SMF Data Unload Utility (RACFADU).

SMF Audit events

1. No access granted:

```
<event>
  <eventType>PERMIT</eventType>
  <eventQual>SUCCESS</eventQual>
  <prodName>RACF</prodName>
  <details>
    <resName>DEFINE.MDISK</resName>
    <specified>CLASS(VMCMD) ID(SYSOP1) ACCESS(READ)</specified>
  </details>
</event>
<event>
  <eventType>ACCESS</eventType>
  <eventQual>INSAUTH</eventQual>
  <details>
    <violation>Y</violation>
    <evtUserId>SYSOP1</evtUserId>
    <resName>DEFINE.MDISK</resName>
    <request>UPDATE</request>
    <grant>READ</grant>
    <class>VMCMD</class>
  </details>
</event>
```

2. Access granted:

```
<event>
  <eventType>PERMIT</eventType>
  <eventQual>SUCCESS</eventQual>
  <prodName>RACF</prodName>
  <details>
    <resName>DEFINE.MDISK</resName>
    <specified>CLASS(VMCMD) ID(SYSOP1) ACCESS(UPDATE)</specified>
  </details>
</event>
<event>
  <eventType>ACCESS</eventType>
  <eventQual>SUCCESS</eventQual>
  <prodName>RACF</prodName>
  <details>
    <violation>N</violation>
    <evtUserId>SYSOP1</evtUserId>
    <resName>DEFINE.MDISK(A) DEFINE MDISK 200 100 100 VOL001</resName>
    <class>VMXEVENT</class>
  </details>
</event>
```

Audit Records for LINK and MDISK

You can use RACF to audit links to z/VM minidisks using profiles in the VMMDISK resource class. The following events can be audited:

LINK command
A user's attempt to link to another user's minidisk.

MDISK event
A user linking to his or her own minidisk. MDISK events occur at logon time when the user's MDISK directory statements are being processed or when the user issues a LINK command for a self-owned minidisk.

The audit records for LINK and MDISK contain the access mode in which the minidisk has been accessed. If an MDISK request has been downgraded by RACF due to a mandatory access control (MAC) failure, then the audit record indicates a mode of RR. An MDISK request is downgraded when a user requests a certain access authority but a lower access authority is granted.

For example, USERA has the following statement in the CP directory:

```
MDISK 191 3380 000 010 191DSK MR
```

In this example, two security labels are defined—CONF and RESTRICT—and RESTRICT dominates CONF. The profile for USERA.191 contains a security label of CONF. If USERA logs on at RESTRICT, read/write access is not given. Since RESTRICT dominates CONF, read/only access is given by RACF. In this case, the audit record indicates that the user was granted READ access.

If CP denies a LINK request after RACF authorizes it, an audit record is created with a mode of XX.

Audit Records for Real Devices

You can use RACF to audit connections to z/VM real devices using either the RDEVCTRL system event or the profiles in the VMDEV resource class. When auditing VMDEV profiles, the can specify auditing under the following conditions:

ALWAYS
NEVER
SUCCESSES
FAILURES
DEFAULT - Auditing is specified for each profile as AUDIT(*access-attempts*[(*audit-access-level*)]), which defaults to FAILURES(READ). Therefore, by default, audit records are produced for any failing authorization checks on any profile in the RDEVCTRL class.

Although auditing the RDEVCTRL system event does not have the same granularity of control as auditing the VMDEV profiles, it does have the advantage of writing an audit record even if authorization checks are not being made because the RDEVCTRL system event is not being controlled.

The audit of the following commands:

- **ATTACH** (a user's attempt to connect to a real device)
- **GIVE** (a user's attempt to transfer control of a real device)

is implemented in the command router and only indicates whether the user has the required privilege class (B) to issue the command.

Auditing START of a Real Printer

Changing the SECLABEL of a real CP printer is done with the CP START command. If the installation wants to audit changes made to security labels for CP printers, the auditor must turn on auditing for START. The VMXEVENT audit record contains the SECLABEL of the command issuer and the new SECLABEL of the printer.

Auditing CP Printing of Files

Files printed on a CP printer can be audited by turning on audit for UTLPRINT.

Auditing for OpenExtensions VM

RACF writes audit records for the OpenExtensions VM auditable events in SMF type 80 records. File owners and auditors can establish separate sets of auditing rules, and can also specify auditing for each file and directory. For more information on these event codes, see *z/VM: RACF Security Server Macros and Interfaces*.

Classes that Control Auditing for OpenExtensions VM

The following classes are defined to control auditing:

- DIRACC
- DIRSRCH
- FSOBJ
- FSSEC
- PROCESS

No profiles can be defined in these classes. They are for audit purposes only. These classes do not need to be active to be used to control OpenExtensions VM auditing. Activating the classes has no effect on auditing or authorization checking.

Each of the classes controls auditing for OpenExtensions VM in a particular way. You can use the SETROPTS LOGOPTIONS command to specify the logging options. The descriptions that follow define the type of auditing each class controls.

The classes are:

DIRACC
Controls auditing for access checks for read/write access to directories:

Audit event codes:
29, 56

DIRSRCH
Controls auditing of directory searches:

Audit event code:
28

Attention:
Auditing directory searches may degrade BFS and RACF performance because directory searches are performed so frequently.

FSOBJ
Controls auditing for all access checks for file system objects except directories via SETROPTS LOGOPTIONS and controls auditing of creation and deletion of file system objects (including directories) via SETROPTS AUDIT.

For object access:

Audit event codes:
30, 56

For object create and delete or name change:

Audit event codes:
41, 42, 43, 45, 47, 48, 53, 54

FSSEC
Controls auditing for changes to the security data (file owner, file mode, and audit options) for file system objects:

Audit event codes:
31, 33, 34

PROCESS
Controls auditing of changes to the UIDs and GIDs of processes

Audit event codes:
36, 49, 50, 51, 52

Activating Auditing for Access Attempts by Class

If you have the AUDITOR attribute, you can audit attempts to access resources in the OpenExtensions-related classes according to the option selected.

For example, the following command specifies that auditing be done for all attempts to access OpenExtensions BFS files, which are audited in the FSOBJ class.

```
SETROPTS  LOGOPTIONS(ALWAYS(FSOBJ))
```

In this case, auditing is done every time a user attempts to access an OpenExtensions file, regardless of the auditing options specified within the file.

You can specify that auditing be done for the following conditions:

ALWAYS
All attempts to access resources protected by the class are audited.

NEVER
No attempts to access resources protected by the class are audited. (All auditing is suppressed.)

SUCCESSES
All successful attempts to access resources protected by the class are audited.

FAILURES
All failed attempts to access resources protected by the class are audited.

DEFAULT
Auditing is controlled by the auditing options specified within the file or directory.

Note: The SUCCESSES and FAILURES operands result in auditing in addition to any auditing specified in the file or directory. In contrast, the ALWAYS and NEVER operands override any auditing specified in the file or directory.

LOGOPTIONS(DEFAULT(*)) is in effect at RACF initialization.

To reset logging to be controlled by options in the files or directories, specify LOGOPTIONS(DEFAULT(*)) on the SETROPTS command.

Specifying Audit Options at the File and Directory Levels

In addition to the class auditing options, you can specify auditing options at the file system object level. This corresponds to setting logging options within a RACF profile. Audit information is carried along with the file in the byte file system (BFS) instead of in a RACF profile. There are two sets of audit options: one that contains the owner's logging options and one that contains the auditor's logging options.

You can specify audit options for each of the access types, where the access types are defined as READ, WRITE, and SEARCH/EXECUTE. For each access type, you can specify the following audit options:

- Don't audit
- Audit successes
- Audit failures
- Audit successes and failures

The owner and auditor audit settings are "ORed" when RACF decides whether to perform auditing. For example, when a write open attempt to a file fails, if the owner option is `don't audit` but the auditor options say to audit all write access attempts, RACF creates an audit record.

The BFS owner and auditor file level options correspond to the AUDIT and GLOBALAUDIT settings that can be defined for a RACF general resource profile, although RACF commands are not used to change the audit options of a BFS file. For details, see the description of the AUDIT and GLOBALAUDIT options of the RDEFINE and RALTER commands in *z/VM: RACF Security Server Command Language Reference*. The file level audit options are honored in the same manner as the RACF profile level audit options. For example:

- If SETROPTS LOGOPTIONS(SUCCESSES(FSOBJ)) is in effect, the file level options are honored in addition to SUCCESSES.
- If SETROPTS LOGOPTIONS(ALWAYS(FSOBJ)) is in effect, the file level options are overridden.

For a complete description of SETROPTS LOGOPTIONS, see *z/VM: RACF Security Server Command Language Reference*.

Using the Default Audit Options

When a file or a directory is created, default audit options are assigned. Different defaults are set for owners and auditors.

The default audit options are:

Owner audit options:
For all access types, audit all failed access attempts

Auditor audit options:
For all access types, don't audit

Changing the Audit Options

OpenExtensions BFS files contain a set of owner-controlled audit settings and a set of auditor-controlled audit settings, just as RACF profiles do. These can be managed using the chaudit() C++ library routine, which uses the BPX1CHA callable service. For more information, see *z/VM: OpenExtensions Callable Services Reference* and *XL C/C++ for z/VM: Runtime Library Reference*.

Restrictions

There are restrictions on who can change the audit options.

- For owner audit options, you must be the owner of the file or a superuser.
- For auditor audit options, you must have the RACF AUDITOR attribute. You can then change the auditor audit options for any file in the file system.

  For a RACF auditor, neither search nor read access to the directories used to locate the file are required and no other authority to the file is needed. You can list the audit options for the objects in a directory using the OpenExtensions `ls` command with the `-W` option. For information about the `ls` command, see *OpenExtensions for z/VM Command Reference*.

Processing Audit Records on z/VM

At initialization, RACF uses the SMF CONTROL file to determine on which of two minidisks to record SMF records. When RACF fills up the minidisk on which it began recording, it uses the SMF CONTROL file to determine the location of the alternate minidisk.

When it switches minidisks, RACFVM updates the CURRENT field in the SMF CONTROL file (on RACFVM's A-disk) to reflect the minidisk that it is now recording on.

Note: If the default addresses, file modes, and CPU IDs specified in the file shipped with RACF do not fit your needs you can edit the SMF CONTROL file and change them.

Following is the default SMF control record contained in the SMF CONTROL file:

```
CURRENT 301 K PRIMARY 301 K SECONDARY 302 K 10000 VMSP CLOSE 001 SEVER NO 0 RACFSMF
```

In this record:

- The virtual addresses of the SMF minidisks are 301 and 302
- The filemode is K
- The default maximum buffer size for the SMF DATA file is 10000
- VMSP is the ID of the CPU where RACF generates the SMF records. RACF limits the CPU ID to four characters. It is used as an identifier for SMF records and should not be confused with the larger CPU ID in z/VM systems.
- CLOSE *nnn* specifies the number of audit records RACF buffers before they are written to the SMF file. You can specify 000-999; the default value is 001.

  The CLOSE 001 ensures that the audit requests processed by RACF are not buffered before being written to the SMF data file.

  If you specify CLOSE 000, the file is not explicitly closed by RACF; CMS writes the audit records when the internal buffer is full.

  If *nnn* is large, RACF can write more audit records per second, thereby improving system performance. However, more audit records could be lost during a system failure.
- The SEVER keyword is initially set to NO. If you choose to set SEVER to YES, RACF will:
  - Terminate server startup if it detects a problem that will prevent RACF from starting SMF recording.
  - Sever the path between CP and RACF when the SMF disks are full, and RACF is unable to continue recording SMF records.

  Before setting SEVER to YES, you should consider its effect on system availability.
- The 0 is a flag used by RACF. Do not alter it.
- RACFSMF is the user ID that is autologged when the 301 or 302 minidisk is filled.

Attention:
If you edit the SMF CONTROL file, you must not alter the format of the control record: • A single space must separate operands. • The SMF CONTROL file must be a fixed block logical record length of 100.

Figure 11 on page 42 shows how SMF records can be used.

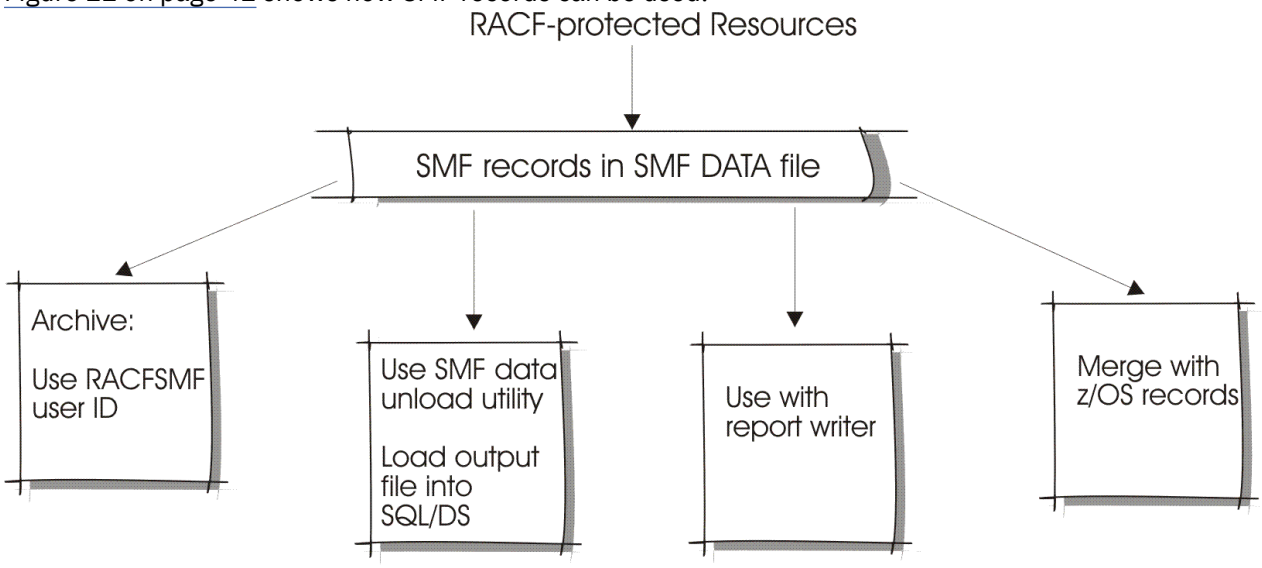

Figure 11. Creating Audit Records

Audit records are written to the SMF DATA file. You can use the records from this file in a variety of ways:

- To use the files with the RACF SMF data unload utility, see Chapter 3, “RACF SMF Data Unload Utility (RACFADU),” on page 49
- To use the files with the RACF report writer, see Appendix A, “The RACF Report Writer,” on page 91
- To merge these records with SMF records created for an z/OS system, see “Merging SMF Records Produced for z/VM with SMF Records Produced for z/OS” on page 43
- To archive the records, see “Archiving Audit Records on z/VM” on page 43.

Merging SMF Records Produced for z/VM with SMF Records Produced for z/OS

Although the content of the RACF audit records is the same in z/VM as it is in z/OS, the record format is slightly different. Therefore, if you want to merge the SMF records produced by RACF for z/VM with those produced by RACF for z/OS, the z/VM records must be reformatted.

SMFCONV is a program that reformats the RACF for z/VM SMF records, and writes them to a file that can be transferred to z/OS for processing by the RACF report writer. SMFCONV is on the RACF service machine's 305 disk.

To use SMFCONV, enter:

```
SMFCONV [fn ft fm]
```

If no file is specified, SMFCONV uses SMF DATA * as input. Otherwise, the file specified in the command is the input file. Output is written to the file SMF RFMT.

SMFCONV does not erase SMF RFMT before writing to it. Therefore, each use of SMFCONV adds to what is already in the file.

Attention:
To run SMFCONV, you need to access the: • SMFCONV module • Audit record input file

Archiving Audit Records on z/VM

On z/VM, RACF provides an EXEC called SMFPROF to allow you to archive audit records:

- On a regular basis
- When the SMF minidisk is full

To use the EXEC you must perform the following steps.

Note: These instructions also apply if you have multiple RACF service machines, as there is only one RACFSMF user ID. You will, however, receive several SMF audit files (one from each service machine).

1. Create a RACFSMF user ID as described in *RACF Migration and Planning*. The RACFSMF user ID must be defined in the CSTCONS table if you archive on a regular basis.
2. Copy the SMFPROF EXEC from the RACFVM 305 disk to the RACFSMF 191 disk with a file name PROFILE and a file type EXEC.
3. Create an SMF archive disk. The SMF archive disk can be either a minidisk or an SFS directory. For a minidisk, create a 192 MDISK definition for the RACFSMF user ID. For an SFS directory, enroll a user ID and create a directory in an SFS file pool that will be used as the SMF archive disk. For either minidisk or SFS, be sure to allow enough space for the data you expect to receive, because installation auditing requirements vary.
4. Permit RACFSMF to RACFVM's 301 and 302 disks with ALTER access, and to RACFVM's 191 disk with READ access.

5. Decide whether to archive the SMF records on a regular basis or only when the SMF minidisk is full.

Archiving on a Regular Basis

If you want to archive on a regular basis, edit the PROFILE EXEC in the following way:

1. Using the SMFDISK operand, specify either the virtual address of the minidisk or the identifier of the SFS directory on which you want to keep the archived records. The default is the 192 minidisk.

   ```
   SMFDISK  = 192
   ```

   Note: If you specify a disk other than 192, you must create a directory entry to correspond to that disk.

   To specify an SFS directory, you can specify either the full name of the directory or the shorthand notation for the directory. For example:

   ```
   SMFDISK = 'VMSYSU:RACFSMF.AUDIT'
   ```

   or

   ```
   SMFDISK = '.AUDIT'
   ```

   Note: If shorthand notation is used to specify the directory, the file pool used will be the default file pool set with the SET FILEPOOL command, and the file space used will be the default file space set with the SET FILESPACE command or the RACFSMF file space, if the SET FILESPACE command was not used to set a default file space.
2. Specify the SMFFREQ and SMFDAY operands to reflect the interval you choose to archive.

   `SMFFREQ = 'WEEKLY'`

   WEEKLY is the default for how often you want to archive the SMF records. The alternatives are MONTHLY, DAILY, and AUTO.

   `SMFDAY = 'MONDAY'`

   MONDAY is the default for the day that you want the archiving to take place. The alternatives are the other days of the week.
3. The RACFSMF user ID must be defined in the CSTCONS table and you must specify:

   `SMFSWTCH = 'YES'`

   YES indicates that the RACFSMF user ID can issue the SMF SWITCH command, which switches SMF recording from one SMF minidisk to the other and continues the PROFILE EXEC that archives the SMF data.
4. Establish a procedure whereby the RACFSMF user ID is autologged everyday. The XAUTOLOG statement for the RACFSMF userid must supply the user IDs of the service machines to be archived as console data.

   For example, if the RACF service machine user IDs are RACFVM, RACFVM1, and RACFVM2, an XAUTOLOG statement would appear as:

   ```
   XAUTOLOG RACFSMF #RACFVM RACFVM1 RACFVM2
   ```

   Note: The symbol *#* has special restrictions. For example, it can appear as a logical line end, thereby causing the system to attempt to execute RACFVM (in the example) as a command. For additional information on these restrictions, refer to *CP Command and Utility Reference*.

   For an AUTOLOG (with SET PASSWORD AUTOLOG INCLUDE), if the RACF service machine user IDs are RACFVM, RACFVM1, and RACFVM2, the statement would appear as:

   ```
   AUTOLOG RACFSMF <password> RACFVM RACFVM1 RACFVM2
   ```

   For an AUTOLOG (with SET PASSWORD AUTOLOG SEPARATE), if the RACF service machine user IDs are RACFVM, RACFVM1, and RACFVM2, the statement would appear as:

```
AUTOLOG RACFSMF RACFVM RACFVM1 RACFVM2
```

Archiving Only When the SMF Disk Is Full

If a set interval is not important to your installation, set up the RACFSMF profile so that a RACF service machine can XAUTOLOG the RACFSMF user ID when the SMF minidisk fills up.

Note: There is no additional setup required for multiple RACF service machines. RACF does this automatically.

Edit the PROFILE EXEC in the following way.

- Using the SMFDISK operand, specify either the virtual address of the minidisk or the identifier of the SFS directory on which you want the archiving to take place. The default is the 192 disk.

  ```
  SMFDISK  = 192
  ```

  Note: If you specify a disk other than 192, you must create a directory entry to correspond to that disk.

  To specify an SFS directory, you can specify either the full name of the directory or the shorthand notation for the directory. For example:

  ```
  SMFDISK = 'VMSYSU:RACFSMF.AUDIT'
  ```

  or

  ```
  SMFDISK = '.AUDIT'
  ```

  Note: If shorthand notation is used to specify the directory, the file pool used will be the default file pool set with the SET FILEPOOL command, and the file space used will be the default file space set with the SET FILESPACE command or the RACFSMF file space, if the SET FILESPACE command was not used to set a default file space.
- Specify:

  ```
  SMFSWTCH = 'NO'
  ```

  This indicates that the RACFSMF user ID cannot issue the SMF SWITCH command, which switches SMF recording from one SMF minidisk to the other.

  RACFVM autologs the RACFSMF user ID automatically, and the RACFSMF user ID does not need to be in the CSTCONS table.
- Specify SMFFREQ='AUTO' so that RACFSMF always archives whenever RACFVM invokes it through an xautolog.

On z/VM, the RACRPORT EXEC uses the RACFRW CONTROL file that contains control statements for the report writer. To ensure that the report writer has access to the SMF data (record types 20, 80, and 81) it requires, you must be linked to the SMF minidisk before you use the report writer command and subcommands. If you are using the RACFSMF user ID, link to the minidisk that contains the archived files.

Note: z/VM does not use record type 30.

Maintaining Auditability for Shared User IDs on z/VM

Audit records help maintain accountability for shared user IDs. RACF creates audit records to identify a surrogate user who tries to access a resource or issue a z/VM command, diagnose, or system function.

When an audit record is created using audit specifications in a resource profile, the report writer:

- Indicates whether a surrogate relationship exists for the user ID that accessed the resource
- Tells what the surrogate user ID is

When someone attempts to logon to a shared user ID, the audit records identify the surrogate user, whether the attempt succeeds or not. If someone attempts to logon directly to a shared user ID, the audit record logs information the auditor may need to use if the attempt fails.

After a surrogate user logs on to a shared user ID successfully, all audit records created by RACF as a result of subsequent activity on the shared user ID identify the surrogate user who caused the event to occur. These audit records may be produced as a result of:

- Audit specifications in a resource profile or LOGOPTIONS setting for a resource class
- Auditing various z/VM events through the use of VMXEVENT profiles. For more information on these records, see *z/VM: RACF Security Server Macros and Interfaces*.

Logon Audit Records for Shared User IDs

RACF creates one Event 1 (LOGON) SMF record each time a user attempts to logon to the system. For sample report writer output, see "Sample Report Writer Output for Shared User IDs" on page 129.

- When a surrogate user attempts to log on to a shared user ID, the record contains a log string (LOGSTR=) of "LOGON BY". In most cases, this record contains information on both the shared and the surrogate user ID. However, if the attempt fails because the surrogate user could not be verified successfully, the record contains only information on the surrogate user.

  Although this record appears as a standard record for an unsuccessful logon attempt, the log string of "LOGON BY" indicates that the user verification failed during a shared logon attempt.
- When a user attempts a standard logon (direct LOGON to a non-shared user ID), RACF creates an audit record with a log string of "LOGON".
- When a user attempts to logon directly to a user ID defined as shared, RACF creates an audit record with a log string of "LOGON".

  For information about the LOGSTR= keyword, see *z/VM: Security Server RACROUTE Macro Reference*.

You can activate audit specifications in the SURROGAT class profile to audit direct logons to shared user IDs. By default, the RDEFINE command tells RACF to produce an audit record if a READ access violation occurs to the profile. Therefore, for attempts to logon to a shared user ID directly, the audit records only show failed attempts. If you want an audit record created when a user successfully logs on to a shared user ID directly, use the RALTER command:

```
RALTER SURROGAT LOGONBY.user AUDIT(ALL(READ))
```

This also audits successful shared logons to the shared user ID.

Maintaining Auditability from RACROUTE Applications

An application that issues RACROUTE requests on behalf of another user ID is responsible for maintaining a proper audit trail if that user ID is a shared ID. The application should issue a Diagnose 26C subcode 4 to determine if there is a surrogate relationship for the user ID and to identify the surrogate user ID. If a surrogate user ID exists, the application may audit the surrogate user by:

- Using a log string

  If appropriate, the application can place the surrogate user ID into the log string for a given RACROUTE request type. The format of the log string is defined and documented by the application.
- Building a surrogate token

  If the application performs RACROUTE request types under the end-user's ACEE (for example, a third party RACROUTE), the application can modify its code to issue a RACROUTE REQUEST=VERIFY for the shared user ID by providing:

  – The shared user ID on the USERID= keyword
  – The surrogate user ID (returned by Diagnose 26C subcode 4) on the SUSERID= keyword

  Note: You must specify PASSCHK=NO on this VERIFY request for surrogate checking to succeed. If password verification on the surrogate user ID is required:

  1. Perform a RACROUTE REQUEST=VERIFYX on the surrogate user, providing password information.

2. Request the token to be returned to your program by using the TOKNOUT= keyword. RACF returns a token for this request that can be used on the STOKEN= keyword of the RACROUTE REQUEST=VERIFY, rather than specifying the SUSERID= keyword.

This creates an ACEE that contains surrogate user information. Providing this ACEE on subsequent RACROUTE requests issued on behalf of the shared user ID results in the same auditability that RACF provides for shared user IDs.

For sample code that uses this function and for details on using RACROUTE, see *z/VM: Security Server RACROUTE Macro Reference*.

Things to Consider:

If an application does not maintain a proper audit trail for shared user IDs, use the following procedures if you need to know whether a shared user ID was associated with a particular RACF audit record:

- If the application uses RACROUTE to audit certain application-specific events through RACF, the record contains a timestamp. In this case, you can:
  1. Search the RACF audit log backwards to find the LOGON record for the appropriate user ID.
  2. Determine if the user ID was logged onto as shared.
  3. Identify the surrogate user ID.
- If the application performs its own logging without using RACF and the audit record contains a timestamp, you can use the same procedure.

Special LOGON BY Considerations for Auditors

You need to consider restrictions for RACROUTE and with batch applications when using the LOGON BY function.

RACROUTE Restriction for Release=1.8.2 Keyword

Because the SUSERID and STOKEN keywords were not added to RACROUTE until release 1.9, RACROUTE requests with RELEASE=1.8.2 coded cannot be used for shared user IDs. A third party RACROUTE REQUEST=AUTH (with RELEASE=1.8.2) performed on behalf of a user ID that is defined as shared in the SURROGAT class is not audited as an access attempt by a shared user ID.

Auditability Restrictions with Batch Applications

Shared user IDs present an auditability concern when used in conjunction with VM's alternate user ID function, which is implemented by Diagnose D4.

- VM's batch processing does not consider that a user submitting a job may be shared.
- Because jobs are submitted using SPOOL files, it is possible that the submitting user has logged off before the SPOOL file gets processed by the batch machine. In this case, the batch machine does not have the option of issuing a Diagnose 26C subcode 4 to obtain the surrogate user ID. Therefore, if worker machines work on behalf of shared user IDs, the result is a loss of auditability for the user ID that is logged on to the alternate user ID as shared.

An installation can decide whether shared user IDs can be used as alternate user IDs.

- If the installation chooses to ignore this auditing concern, no action is necessary.
- If the installation wants to prevent a shared user ID from submitting a batch job, you can do this by:
  1. Turning on control for the Diagnose D4 event in the currently active VMXEVENT profile. This ensures that RACF controls the use of Diagnose D4.
  2. Defining the VMBATCH profile for that shared user ID so that no user ID can access it. This prevents a Diagnose D4 from successfully specifying the shared user ID as an alternate user ID (see *CP Programming Services* for a description of Diagnose D4).

Note: An installation may want to enforce this restriction only for certain batch applications. In this case, you can create individual VMXEVENT profiles for the user IDs running these batch applications without Diagnose D4 being controlled. If Diagnose D4 is controlled in the system-wide VMXEVENT profile, the batch restriction is bypassed only for those few applications.

If an installation wants to enforce this restriction only on certain shared user IDs, you can modify only the VMBATCH profile for those specific shared user IDs, assuming Diagnose D4 is being controlled.

Attention:
If Diagnose D4 is *not* controlled by a given installation, this type of auditability is not possible for that installation when the SURROGAT class is activated, unless the appropriate steps are taken.

Chapter 3. RACF SMF Data Unload Utility (RACFADU)

RACF audit data is a record of an installation's security-relevant events. This data is used to verify the effectiveness of an installation's security policy, determine whether the installation's security objectives are being met, and identify unexpected security relevant events.

You can use the RACF SMF data unload utility to create a sequential file from the security relevant audit data. You can use the file in several ways. It can be:

- Viewed directly
- Used as input to your own programs
- Manipulated with sort/merge programs
- output to an XML-formatted file for viewing on a web browser
- Used as input to a database management system to produce reports tailored to your requirements

The RACF SMF data unload utility processes the following types of SMF records created by RACF for z/VM:

Type 80
Resource access

No subtypes in record

Type 81
RACF initialization

No subtypes in record

Type 83
LDAP - Subtype 3

remote audit - Subtype 4

To correlate the RACF audit data with the unloaded data see the description of the SMF records contained in *z/VM: RACF Security Server Macros and Interfaces*.

For more details about working with subtype 3 LDAP audit records, see *z/OS Integrated Security Services LDAP Server Administration and Use*.

Using the RACF SMF Data Unload Utility

z/VM installations use the RACFADU EXEC to execute the SMF data unload utility.

You can execute the IRRADU00 utility either by panel invocation or command invocation. For details, see "Panel Invocation of RACFADU" on page 50 and "Command Invocation of RACFADU" on page 51.

RACFADU Setup

Before unloading the SMF records produced by RACF you must:

1. Logon to a virtual machine that has read access to the RACF service machine's 305 disk, and to the minidisk containing the SMF records to be unloaded (this may be a RACF service machine's 301 or 302 minidisk).
2. IPL the RACF service machine's 490 minidisk.
3. Access RACF's 305 disk as file mode B.
4. Link the output minidisk as R/W.
5. Have a R/W minidisk accessed as file mode A.
6. Ensure that there is adequate free space on the output minidisk to contain the utility output file.

© Copyright IBM Corp. 1993, 2024

The size of the output file is roughly estimated as twice the size of the used portion of the SMF recording disk.

Panel Invocation of RACFADU

Begin the exec by entering RACFADU on the command line. The input panel appears on your screen. Figure 12 on page 50 illustrates the RACFADU input panel.

```
                RACF SMF Unload Utility - Input Panel


    Virtual address of input SMF data minidisk                bbbb

    Virtual address of output minidisk                        cccc

    Filename and filetype of sequential output file           fname    ftype

    Filename and filetype of XML easily readable output file  xrname   xrtype

    Filename and filetype of XML compressed output file       xcname   xctype


                 PF1 = Help    PF2 = Execute   PF3 = Quit
                        ENTER = Verify input fields

 ====>
```

Figure 12. Input Panel for RACFADU

The user must supply the following values:

bbbb
The virtual address of the minidisk which contains the SMF records to be unloaded. Typically, this will be the 301 or 302 disk of a RACF service machine, but it should not be the currently active SMF recording minidisk. RACFADU assumes that the file name and file type of the SMF records to be processed is:

```
SMF DATA
```

which is the file name and file type of the SMF records recorded by RACF.

cccc
The virtual address of the output minidisk where the unloaded output will be written. This must be a CMS formatted minidisk with enough free space to contain the output file which will be approximately twice as large as the input file. This minidisk must be linked R/W.

This is a required input field.

fname ftype
The file name and file type of the output file. RACFADU OUTPUT is the default. You can supply another file name or file type.

If the output file you specify already exists, the utility changes the file type of the existing file. For example, if the default file (RACFADU OUTPUT) exists on the output minidisk, the existing file is copied to a file named RACFADU OUTPUT1 on the same disk. It overlays any previous RACFADU OUTPUT1 file. If the file type is 8 characters long, the last character is changed to a 1.

xrname xrtype
The filename and filetype which is asigned to the XML easily readable output file. If the file already exists on the output minidisk, the existing file will be renamed to a file on the same disk with a filetype having an appended "1" (for example, if RACFADU XMLFORM exists it will be copied to RACFADU XMLFORM1 overlaying any previous RACFADU XMLFORM1).

xcname xctype
The filename and filetype which is asigned to the XML compressed output file. If the file already exists on the output minidisk, the existing file will be renamed to a file on the same disk with a filetype having an appended "1" (for example, if RACFADU XMLOUT exists it will be copied to RACFADU XMLOUT1 overlaying any previous RACFADU XMLOUT1).

The input values entered on the panel are saved and reappear the next time you invoke RACFADU. After you have entered your input in the required fields, press one of the following keys. The meaning of the ENTER key and the PF key definitions are:

Key
Meaning

Enter
Verify user screen input as to containing required fields. Messages will be issued in a top/down fashion without the unload being performed.

PF1
Display help screen explaining purpose. Use ALL function once in help panel to display more detailed information about user input fields.

PF2
This is the execute key. Once pressed, all input fields will be validated. If all required fields are supplied and all user input is valid, the unload utility will be invoked.

PF3
Terminates RACFADU processing.

Command Invocation of RACFADU

Your installation may want to run the IRRADU00 utility without interactive processing. To start the utility automatically, you can invoke the utility from a command line or a user-written exec, but input parameters must be correctly specified. The command invocation fields are similar to the panel invocation fields. All required parameters must be valid or the SMF data unload utility will not be invoked.

Syntax for command invocation

```
RACFADU bbbb cccc  [(options...[])]

Options:
[OUTFN filename]
[OUTFT filetype]
[OUTXRN filename]
[OUTXRT filetype]
[OUTXCN filename]
[OUTXCT filetype]
```

The explanation of the input fields follows:

bbbb
Virtual address of the input SMF data minidisk.

This is a required parameter.

cccc
Virtual address of the output R/W minidisk.

This is a required parameter.

OUTFN *filename*
File name of output sequential file (default: RACFADU)

OUTFT *filetype*
File type of the output sequential file. (default : OUTPUT)

OUTXRN *filename*
File name of output XML easily readable file.

OUTXRT *filename*
File type of output XML easily readable file.

OUTXCN *filename*
File name of output XML compressed.

OUTXCT *filename*
File type of output XML compressed.

Command Invocation Return Codes

To determine if the SMF data unload utility successfully executed, check the return code. A return code of 0 indicates successful utility execution. A return code of 16 indicates that the utility did not execute. It is issued with error messages indicating the reason for failure.

RACF SMF Data Unload Utility Messages

Messages issued by the RACF SMF data unload utility (IRR67xxx messages) are placed in a file named RACFADU MESSAGES on the user's A-disk. The IRR67xxx messages are documented in *z/VM: RACF Security Server Messages and Codes*.

Messages from RACFADU appear on the input screen and are documented in *z/VM: RACF Security Server Messages and Codes*. Messages issued by the RACFADU EXEC begin with RPIADU. The messages issued by the RACFADU EXEC are also documented in the HELP which is available by pressing PF1 on the RACFADU input panel. The help contains the invocation parameters and a list of the messages, along with message explanations and actions that you should take.

Using the Output from the SMF Data Unload Utility

The output file from the RACF SMF data unload utility can be:

- Viewed directly
- Used as input to your own programs
- Manipulated with sort/merge utilities
- Used as input to a database management system so you can produce reports tailored to your requirements
- Viewed using a web browser

Sort/Merge Programs

The RACF SMF data unload records include type 80, 81, and 83 SMF records. If you want a subset of the records, you can use a standard utility such as DFSORT/CMS to select them.

Relational Databases

You can use the power of a relational database management system (DBMS), such as SQL/DS, to process the RACF SMF data unload records. Refer to the following section for details.

XML

RACF SMF data records can be output as XML and then viewed using a web browser. This can give you a better view of the data as well as use colors to differentiate information. For more details, see “Using the RACF SMF data unload utility to generate XML documents” on page 57.

Using the SMF Data Unload Utility Output with SQL/DS

The records produced by the RACF SMF data unload utility are designed to be processed by the SQL/DS load utility or its equivalent. The definition and control statements that let SQL/DS use the records are as follows:

- IRRADUTB SAMPLE

  Sample data definition language (DDL) statements to define the relational representation of the audit information and sample SQL/DS definitions that perform database and index creation.
- IRRADULD SAMPLE

  Sample control statements for the SQL/DS load utility that map the output from the RACF SMF data unload utility.
- IRRADUQR SAMPLE

  Sample structured query language (SQL) queries that perform useful data inquiries.

For complete information on SQL/DS, see:

- *SQL/Data System General Information for IBM VM Systems*
- *SQL/Data System Database Administration for IBM VM Systems*
- *SQL/Data System System Administration for IBM VM Systems*
- *SQL/Data System SQL Reference for IBM VM Systems and VSE*

Steps for Using RACF SMF Data Unload Utility Output with SQL/DS

To create and manage the SQL/DS database containing output from the RACF SMF data unload utility, you must:

1. Create one or more SQL/DS DBSPACEs.
2. Create SQL/DS tables.
3. Create the SQL/DS indexes.
4. Load data into the tables.
5. Reorganize the indexes (optional).
6. Delete table data (optional).

The first three steps are initial setup, and you can choose to run them once. When you get new data to import into the SQL/DS database, you erase your current table data. You then reload and reorganize your indexes.

The following sections show examples of the SQL/DS utility input for these functions.

Creating a SQL/DS DBSPACE

SQL/DS stores tables and indexes on tables in DBSPACEs. A DBSPACE is a logical allocation of space in the database. For more information see *SQL/DS System Administration*.

Creating the SQL/DS Tables

After the DBSPACE is created, SQL statements that define the tables are executed. Figure 13 on page 54 contains an example of the SQL statements required to create a table for the JOBINIT record.

The IRRADUTB SAMPLE file contains examples that create separate tables for each record type produced by the RACF SMF data unload utility. You must supply the user ID (*userid*).

```
CREATE TABLE userid.JOBINIT(
     INIT_EVENT_TYPE          CHAR(8),
     INIT_EVENT_QUAL          CHAR(8),
     INIT_TIME_WRITTEN        TIME,
     INIT_DATE_WRITTEN        DATE,
     INIT_SYSTEM_SMFID        CHAR(4),
     ...
     INIT_UTK_USER_ID         CHAR(8),
     INIT_UTK_GRP_ID          CHAR(8),
     INIT_UTK_DFT_GRP         CHAR(1),
     INIT_UTK_DFT_SECL        CHAR(1),
     INIT_APPC_LINK           CHAR(16)
          ) IN JOBINIT ;
```

Figure 13. Sample SQL Utility Statements Creating a Table

Loading the SQL/DS Tables

Figure 14 on page 54 shows the statements required to load the JOBINIT record. The IRRADULD SAMPLE file contains statements that load all the record types produced by the RACF SMF data unload utility. The sample requires that the output of RACFADU be made into a fixed record length file.

```
 DATALOAD TABLE (JOBINIT)   IF POS(5-12)='JOBINIT '
   INIT_EVENT_TYPE     5-12
   INIT_EVENT_QUAL     14-21
   INIT_TIME_WRITTEN   23-30     NULL IF POS(23-30) ='        '
   INIT_DATE_WRITTEN   32-41     NULL IF POS(32-41) ='          '
   INIT_SYSTEM_SMFID   43-46
   ...
   INIT_UTK_USER_ID    718-725
   INIT_UTK_GRP_ID     727-734
   INIT_UTK_DFT_GRP    736-736
   INIT_UTK_DFT_SECL   741-741
   INIT_APPC_LINK      746-761
  INFILE(IRRADU00);
```

Figure 14. SQL/DS Utility Statements Required to Load the Tables

Note: You can choose not to load some of the tables.

Reorganizing the Indexes in the SQL/DS Database

Queries are processed faster if they are performed against an organized database. SQL/DS provides a utility that allows you to reorganize the indexes on the catalog tables. For more information, see *SQL/DS Database Administration*.

Deleting Data from the SQL/DS Database

Before you reload the database with new data, you should delete the old data. This can be done in several ways:

1. Use the DROP TABLE statement for each table you want to delete.
2. Use the DROP DBSPACE statement for each DBSPACE.
3. Delete all the records in each table.

   To delete the record data shown in Figure 13 on page 54, use the sample SQL statement:

   ```
   DELETE FROM USER01.JOBINIT ;
   ```

SQL/DS Table Names

The IRRADUTB SAMPLE file creates SQL/DS tables for each record type. Table 1 on page 55 provides a useful reference of record type, record name, and SQL/DS table name.

Table 1. Correlation of SQL/DS Table Names and Record Types

Table Name	Column Prefix	Description
JOBINIT	INIT	Job initiation
ACCESS	ACC	Resource access, other than file or directory
ADDVOL	ADV	ADDVOL/CHGVOL
RENAMEDS	REN	Rename data set
DELRES	DELR	Delete resource
DELVOL	DELV	Delete volume
DEFINE	DEF	Define resource
ADDSD	AD	ADDSD command
ADDGROUP	AG	ADDGROUP command
ADDUSER	AU	ADDUSER command
ALTDSD	ALD	ALTDSD command
ALTGROUP	ALG	ALTGROUP command
ALTUSER	ALU	ALTUSER command
CONNECT	CON	CONNECT command
DELDSD	DELD	DELDSD command
DELGROUP	DELG	DELGROUP command
DELUSER	DELU	DELUSER command
PASSWORD	PWD	PASSWORD command
PERMIT	PERM	PERMIT command
RALTER	RALT	RALTER command
RDEFINE	RDEF	RDEFINE command
RDELETE	RDEL	RDELETE command
REMOVE	REM	REMOVE command
SETROPTS	SETR	SETROPTS command
RVARY	RVAR	RVARY command
APPCLU	APPC	APPC session
GENERAL	GEN	General purpose
DIRSRCH	DSCH	Directory search
DACCESS	DACC	Check access to a directory
FACCESS	FACC	Check access to file
CHAUDIT	CAUD	Change audit options
CHDIR	CDIR	Change current directory
CHMOD	CMOD	Change file mode
CHOWN	COWN	Change file ownership
CLRSETID	CSID	Clear SETID bits for a file
EXESETID	ESID	EXEC with SETUID/SETGID

Table 1. Correlation of SQL/DS Table Names and Record Types (continued)

Table Name	Column Prefix	Description
GETPSENT	GPST	Get OpenExtensions process entry
INITOEDP	IOEP	Initialize OpenExtensions process
TERMOEDP	TOEP	OpenExtensions process complete
KILL	KILL	Terminate a process
LINK	LINK	LINK
MKDIR	MDIR	Make directory
MKNOD	MNOD	Make node
MNTFSYS	MFS	Mount a file system
OPENFILE	OPEN	Open a new file
PTRACE	PTRC	PTRACE authority checking
RENAMEF	RENF	Rename file
RMDIR	RDIR	Remove directory
SETEGID	SEGI	Set effective GID
SETEUID	SEUI	Set effective UID
SETGID	SGI	Set GID
SETUID	SUI	Set UID
SYMLINK	SYML	SYMLINK
UNLINK	UNL	UNLINK
UMNTFSYS	UFS	Unmount file system
CHKFOWN	CFOW	Check file owner
CHKPRIV	CPRV	Check OpenExtensions privilege
OPENSTTY	OSTY	Open slave TTY
RACLINK	RACL	RACLINK command
IPCCHK	ICHK	Check IPC access
IPCGET	IGET	Make ISP
IPCCTL	ICTL	R_IPC control
SETGROUP	SETG	Set group
CKOWN2	CKO2	Check owner two files
RACFINIT	RINI	RACF initialization data
CLASNAME	RINC	RACF class data
DSNSAFF	DSAF	Data sets affected by a SECLABEL change

Using the RACF SMF data unload utility to generate XML documents

The records produced by the SMF data unload utility can be formatted as an Extensible Markup Language (XML) document. XML has many advantages over the usual tabular-style data, such as the many applications that can use XML as a format for reading and writing of data. The benefits of XML include:

- A better view of the data. Instead of the tabular format which may be difficult to focus in on the information you're looking for, the XML audit report formats the data for ease of reading and retrieval.
- The display can include different fonts, text emphasis (bold, italic) as well as different colors to differentiate information.
- A complete set of data for each field. The tabular data is limited by space and can be truncated. XML does not have this restriction.
- A view of the audit data that can be tailored to your environment.

XML overview

XML is a flexible language which allows you to tag data and have it displayed in a variety of ways. Many software applications read and write XML data, both in enterprise computing and consumer applications. Therefore, an auditing report using XML can be distributed and analyzed on multiple platforms and operating systems. For more information about XML, see IBM: XML Toolkit for z/OS (https://www.ibm.com/docs/en/zos/3.1.0?topic=descriptions-xml-toolkit-zos).

An XML document which contains the audit report looks like this:

```
<?xml version='1.0'?>
<securityEventLog xmlns='http://www.ibm.com/xmlns/zOS/IRRSchema'>

  <rdf:Description rdf:about=''
                   xmlns:rdf='http://www.w3.org/1999/02/22-rdf-syntax-ns#'
                   xmlns:dc='http://purl.org/dc/elements/1.1/'
                   xmlns:z='http://www.ibm.com/xmlns/zOS'>
    <dc:creator>
      <z:application>SMF Unload</z:application>
      <z:product>z/OS Security Server RACF</z:product>
      <z:fmid>HRF7720</z:fmid>
    </dc:creator>
    <dc:subject>RACF Security Event Log 2003-01-01 04:12:33</dc:subject>
    <dc:language>en</dc:language>
  </rdf:Description>

  <event>
    <eventType>*CONNECT</eventType>
    <eventQual>SUCCESS</eventQual>
    <timeWritten>02:03:01.23</timeWritten>
    <dateWritten>2004-03-28</dateWritten>
    <systemSmfid>SYSA</systemSmfid>
    <prodName>Enterprise Identity Mapping</prodName>
    <prodFmid>HRF7720</prodFmid>
    <details xmlns:d="http://www.ibm.com/xmlns/zOS/EIMSchema">
      <violation>Y</violation>
      <userNdfnd>Y</userNdfnd>
      <userWarning>Y</userWarning>
      <evtUserId>IBMUSER</evtUserId>
      <evtGrpId>SYS1</evtGrpId>
      <authNormal>Y</authNormal>
      <authSpecial>Y</authSpecial>
      <authOper>Y</authOper>
      <authAudit>Y</authAudit>
      <authExit>Y</authExit>
      <authFailsft>Y</authFailsft>
      <authBypass>Y</authBypass>
      <authTrusted>Y</authTrusted>
      <logClass>Y</logClass>
      <logUser>Y</logUser>
      <logSpecial>Y</logSpecial>
      <logAccess>Y</logAccess>
      <logRacinit>Y</logRacinit>
      <logAlways>Y</logAlways>
      <logCmdviol>Y</logCmdviol>
```

```
      <logGlobal>Y</logGlobal>
      <termLevel>934</termLevel>
      <backoutFail>Y</backoutFail>
      <profSame>Y</profSame>
      <term>L0437634</term>
      <jobName>$EIMTEST</jobName>
      <readTime>01:03:04</readTime>
      <readDate>2004-03-28</readDate>
      <smfUserId>SMFUSER</smfUserId>
      <logLevel>Y</logLevel>
      <logLogopt>Y</logLogopt>
      <logSecl>Y</logSecl>
      <logCompatm>Y</logCompatm>
      <logApplaud>Y</logApplaud>
      <usrSecl>HIGHEST</usrSecl>
      <logVmevent>Y</logVmevent>
      <logNonomvs>Y</logNonomvs>
      <logOmvsnprv>Y</logOmvsnprv>
      <authOmvssu>Y</authOmvssu>
      <authOmvssys>Y</authOmvssys>
      <racfVersion>7720</racfVersion>
      <srvrUserId>IBMUSER</srvrUserId>
      <srvrGrpId>SYS1</srvrGrpId>
      <prodId>EIM</prodId>
      <logRauditx>Y</logRauditx>
      <x500Subject>cn=ibmuser,c=us</x500Subject>
      <x500Issuer>cn=PKI CA,c=us</x500Issuer>
      <resName>EIM.MYDOMAIN.CONNECT</resName>
      <class>RAUDITX</class>
      <profileName>EIM.*.CONNECT</profileName>
      <d:api>eimConnect</d:api>
      <d:domainUrl>ldap://some.big.host/ibm-eimdomainname=My Domain,
        c=us</d:domainUrl>
      <d:connectType>SIMPLE</d:connectType>
      <d:bindUser>cn=EIM administrator</d:bindUser>
      <d:certLabel>label</d:certLabel>
      <d:keyRing>keyring</d:keyRing>
    </details>
  </event>
```

Producing XML output

You can have SMF Unload create an XML document by:

- Specifying a filename and filetype on the *xrname* and *xrtype* fields, or *xcname* and *xctype* fields on the RACFADU input panel.
- Specifying a filename and filetype on the OUTXRN and OUTXRT, or OUTXCN and OUTXCT fields on the RACFADU command invocation.

This creates either a compressed form or a more readable form of the XML document.

You can think of the compressed form of output as "raw output", since it is the most basic form of the XML document. While this report takes up the least space, it is not well-suited for reading due to its limited line wrapping and tag justification. In the document, the tags and information are often comprised of one long line in an effort to save space. The more readable form of the report includes better line wrapping, and the tags are justified so that they begin on new lines when necessary. Though it is a more readable form, it takes up more space.

How the XML tag names are derived

The names of the tags and the syntax of the tags are defined by XML schema document. The schema can be used to validate the data contained in an XML document. The tags appear in the order described by the schema documents. The schema document for RACF can be found on the RACF service machine's 305 disk as IRRSCHEM SAMPLE.

In general, the tag names used in RACF are derived from the corresponding SQL/DS field names. The rules for converting a field name to a tag name are:

1. Remove the column name and the first underscore (“_”) from the field name

2. Capitalize the first letter after each of the remaining underscores in the name. The rest of the characters should be lowercase.
3. Remove the underscores from the name

The exceptions to this methodology are as follows:

Table 2. XML naming exceptions

SQL/DS Field Name	**XML Tag Name**
RINI_TERM	riniTerm
SECL_LINK	eventLink
CAUD_REQUEST_WRITE	caudRequestWrite
CAUD_REQUEST_READ	caudRequestRead
CAUD_REQUEST_EXEC	caudRequestExec
SSCL_OLDSECL	oldSecl
<col>logstring	logstr
KTKT_PRINCIPAL	kerbPrincipal
PDAC_PRINCIPAL	pdasPrincipal
any field with RESERVED in the name	**Note:** no XML tag
ACC_NAME	profileName
APPC_NAME	profileName

XML interprets certain characters as having a special meaning, such as "<" and ">". If a value contains one of these special characters, which are listed in Table 4 on page 59, SMF Unload replaces the value with an “entity reference” so that it won't be misinterpreted by an XML parser. Here's an example:

Table 3. XML interpretation of special characters example

Before Value	**After Value**
<subjectDN>cn=John,ou=Smith & Sons,c=us</subjectDN>	`<subjectDN>cn=John,ou=Smith & Sons,c=us,<subjectDN>`

The special characters are:

Table 4. XML special characters substitutions

Character	**Substitution symbol**
<	`<`
&	`&`
>	`>`
“	`"`
'	`'`

It is possible for a single element or value in the XMLOUT or XMLFORM to cause the length of a record to exceed the maximum 8K limit. SMF Unload will break the line into two. If the line break would naturally occur in the middle of a tag or entity reference, SMF Unload splits the line before or after the tag or entity reference so that the tag or entity reference is not broken. What this means is that the data value may include a carriage return or line feed that wasn't originally part of the value. It's up to the application

processing the document to detect this condition and concatenate the two lines before passing the element to an XML parser.

Viewing and working with XML audit reports

The audit report can be viewed on personal computers and workstations using an XML-capable web browser. Many browsers available today have the ability to correctly parse and render XML documents. Therefore, once the audit report is on that system, you can read it as easily as any other web document. Simply bring up a listing of the files and single- or double-click the file to open it in the browser window. The platform documentation can help you discover which applications are able to parse and display XML files.

One thing to note is that to use the XML file on a personal computer, you must first alter the EBCDIC encoding line at the top of the file:

```
<?xml version='1.0' encoding='ebcdic-cp-us' ?>
```

So that it looks like the following:

```
<?xml version='1.0' encoding='ISO8859-1' ?>
```

Event Code Qualifiers

The RACF event code (found in the SMF80EVT field of the SMF record) and the RACF event code qualifier (found in the SMF80EVQ field of the SMF record) are determined during RACF processing. The following sections explain the meaning of each qualifier code by event. Some of these event codes and qualifiers apply only to z/OS systems, but are listed here for completeness.

Event 1(1): JOB INITIATION/TSO LOGON/TSO LOGOFF

This event is logged by RACROUTE REQUEST=VERIFY and RACROUTE REQUEST=VERIFYX.

The explanations of the event code qualifiers for Event 1 are:

0(0)
SUCCESSFUL INITIATION The job began successfully.

1(1)
INVALID PASSWORD The password specified on the job card or at logon is incorrect.

2(2)
INVALID GROUP The user tried to log on or to initiate a job using a group that the user is not a member of.

3(3)
INVALID OIDCARD Operator identification cards are used at the installation, and the data received from the one used does not match that of the user's profile.

4(4)
INVALID TERMINAL/CONSOLE The user is not authorized to the port of entry (POE). There are four kinds of POEs, each with its own profile class: APPCPORT, CONSOLE, JESINPUT, and TERMINAL. One of the following occurred:

- The port of entry is active but the user is not authorized.
- The user is denied access because of conditional days/times in the user profile.
- The user is denied access because of conditional days/times in the class profile (TERMINAL class only).

5(5)
INVALID APPLICATION The APPL class is active, and the user is trying to log on to an application without authorization.

6(6)

REVOKED USER ID ATTEMPTING ACCESS The user ID specified on the logon has been revoked. One of the following occurred:

- The installation-defined limit of password attempts was reached at an earlier time.
- The inactive interval was reached.
- The revoke-date in the user's profile is in effect.
- The RACF administrator revoked the user ID.

The RACF administrator must reset the user ID before the user can log on again.

7(7)

USER ID AUTOMATICALLY REVOKED The user ID has been automatically revoked. The installation-defined limit of password and password phrase attempts was reached.

8(8)

SUCCESSFUL TERMINATION The job completed successfully.

9(9)

UNDEFINED USER ID The user ID specified on the job card or at logon is not defined to the RACF database.

10(A)

INSUFFICIENT SECURITY LABEL AUTHORITY One of the following occurred:

- SETROPTS MLS FAILURES is in effect and the user's security label does not dominate the submitter's security label. Two exceptions are explained under Qualifier 20.
- SETROPTS MLACTIVE FAILURES is in effect and the job card/logon attempt does not specify a valid security label. One exception is explained under Qualifier 21.

11(B)

NOT AUTHORIZED TO SECURITY LABEL The user is not authorized to the security label specified. One exception is explained under Qualifier 22.

12(C)

SUCCESSFUL RACINIT INITIATION The job or user was verified.

13(D)

SUCCESSFUL RACINIT DELETE The job completed or the user logged off.

14(E)

SYSTEM NOW REQUIRES MORE AUTHORITY SETROPTS MLQUIET is in effect. If this is a user verification, the user is not a console operator and does not have the SPECIAL attribute. If this is a job verification, the job is not part of the trusted computing base (TCB). The verification fails.

15(F)

REMOTE JOB ENTRY—JOB NOT AUTHORIZED The submitting node is not authorized to the system; a NODES profile prevents remote job entry. The profile has the format `'submit_node.RUSER.userid'` and has a UACC of NONE.

16(10)

SURROGATE CLASS IS INACTIVE The SURROGAT class is inactive. The job card has a user ID that is different from the submitter's user ID, and there is no password specified. On VM, someone attempted to logon to a shared user ID.

17(11)

SUBMITTER IS NOT AUTHORIZED BY USER The SURROGAT class is active. Either there is no SURROGAT profile for the job card's user ID or the submitter's user ID is not permitted to the profile. On VM, someone attempted to logon to a shared user ID. Either there is no SURROGAT profile for the shared user ID or the user logging on to the shared user ID is not permitted to the SURROGAT profile.

18(12)

SUBMITTER IS NOT AUTHORIZED TO SECURITY LABEL The SECLABEL class is active and there is a security label on the job card. The submitter is not authorized to the security label specified on the job card.

19(13)
USER IS NOT AUTHORIZED TO JOB The JESJOBS class is active, and the user is not authorized to the jobname.

20(14)
WARNING—INSUFFICIENT SECURITY LABEL AUTHORITY One of the following occurred:

- SETROPTS MLS WARNING is in effect and the security label on the job card does not dominate the submitter's security label.
- SETROPTS MLS FAILURES is in effect, the user's security label does not dominate the submitter's, and the user has the SPECIAL attribute.
- SETROPTS MLS FAILURES and SETROPTS COMPATMODE are in effect, the user's security label does not dominate the submitter's, and the submitter's or the job owner's security label is the default.

The verification does not fail.

21(15)
WARNING—SECURITY LABEL MISSING FROM JOB, USER, OR PROFILE One of the following occurred:

- MLACTIVE WARNING is in effect, and the job card or logon attempt did not specify a valid security label.
- MLACTIVE FAILURES is in effect, the user has the SPECIAL attribute, and a valid security label is not specified.

The verification does not fail.

22(16)
WARNING—NOT AUTHORIZED TO SECURITY LABEL The user has the SPECIAL attribute, the security label is SYSHIGH, and the user does not have authority to it. The verification does not fail.

23(17)
SECURITY LABELS NOT COMPATIBLE SETROPTS MLS is not active, the submitter's user ID is different from the user ID on the job card, and the submitter's and the user's security labels are disjoint (neither one dominates the other).

One exception is listed under Qualifier 24.

24(18)
WARNING—SECURITY LABELS NOT COMPATIBLE SETROPTS MLS is not active, the submitter's user ID is different from the user ID on the job card, the submitter's and user's security labels are disjoint, SETROPTS COMPATMODE is in effect, and the submitter's or user's security label is the default. The verification does not fail.

25(19)
CURRENT PASSWORD HAS EXPIRED The user's password has expired for one of the following reasons:

- The installation specification in SETROPTS PASSWORD INTERVAL command
- Creation of the password in the ADDUSER command
- Alteration of the password with the ALTUSER PASSWORD command

26(1A)
INVALID NEW PASSWORD The new password specified may be incorrect because:

- It is all blanks.
- The characters are not all alphanumeric.
- The characters do not match the installation's password syntax rules (set by the SETROPTS PASSWORD command).
- It is the same as a past password (the extent of the past history determined by the SETROPTS PASSWORD HISTORY command).
- It is marked invalid by the installation's password exit.

- It is too soon to change the password (as determined by the SETROPTS PASSWORD MINCHANGE command).

27(1B)
VERIFICATION FAILED BY INSTALLATION The installation exit ICHRIX01 failed the request.

28(1C)
GROUP ACCESS HAS BEEN REVOKED The user's membership to the group specified has been revoked.

29(1D)
OIDCARD IS REQUIRED An OIDCARD is required by the installation but none was given.

30(1E)
NETWORK JOB ENTRY—JOB NOT AUTHORIZED For session types of NJE SYSOUT or NJE BATCH, the verification fails because one of the following occurred:

- The user, group, or security label requirements in the NODES profiles were not met.
- The submitter's node is not valid.
- The reverify check failed.

See *z/VM: RACF Security Server System Programmer's Guide* for details on NJE.

31(1F)
WARNING—UNKNOWN USER FROM TRUSTED NODE PROPAGATED The combination of having a trusted node submit a job with the undefined user ID warrants this logging. The verification does not fail.

For an NJE BATCH job, the submitting user is the NJE undefined user ID. The default NJE undefined user ID is eight question marks (????????), unless it was changed with the SETROPTS JES NJEUSERID command. The submitting node is trusted (its best-fit NODES profile on the receiving node's system has a UACC of at least UPDATE). This profile allows propagation of submitters; however, the undefined user ID does not propagate.

32(20)
SUCCESSFUL INITIATION USING PASSTICKET Logon was achieved using a PassTicket.

33(21)
ATTEMPTED REPLY OF PASSTICKET Logon was rejected because of attempted replay of a PassTicket.

35(23)
USER AUTOMATICALLY REVOKED DUE TO INACTIVITY A user has not logged on or accessed the system for so long that the user ID has become inactive. RACF prevents the user from accessing the system.

36(24)
PASS PHRASE IS NOT VALID A user attempted to access the system specifying a password phrase that is not valid. RACF prevents the user from accessing the system.

37(25)
NEW PASS PHRASE IS NOT VALID Logon was rejected because the new password phrase is not valid.

38(26)
CURRENT PASS PHRASE HAS EXPIRED Logon was rejected because the current password phrase has expired.

40(28)
SUCCESSFUL MULTI-FACTOR AUTHENTICATION Multi-Factor Authentication was successful.

41(29)
FAILED MULTI-FACTOR AUTHENTICATION Multi-Factor Authentication failed.

42(2A)
MULTI-FACTOR AUTHENTICATION UNAVAILABLE Multi-Factor Authentication was unavailable.

Event 2(2): RESOURCE ACCESS

This event is logged by RACROUTE REQUEST=AUTH.

This event is also logged by RACROUTE REQUEST=FASTAUTH if auditing the PROGRAM class. Only qualifiers 0, 1, and 3 are used by RACROUTE REQUEST=FASTAUTH.

The explanations of the event code qualifiers for Event 2 are:

0(0)
SUCCESSFUL ACCESS The user has authorization to the resource.

1(1)
INSUFFICIENT AUTHORITY The user does not have authorization to the resource.

2(2)
PROFILE NOT FOUND—RACFIND SPECIFIED ON MACRO If the request is AUTH, the RACFIND keyword equaled YES on the authorization request, specifying that a discrete profile should exist for the resource. No discrete or generic RACF protection was found.

If the request is FASTAUTH, the program is not controlled and the PADS data sets are open.

3(3)
ACCESS PERMITTED DUE TO WARNING The user does not have proper authority to the resource. However, the resource's profile has the WARNING option and allows the access.

Exceptions:
• PROGRAM class profiles cannot use the WARNING option. • RACLISTed profiles use the WARNING option only if they are RACLISTed by SETROPTS or a RACROUTE REQUEST=LIST that specifies RELEASE=1.8 or later.

4(4)
FAILED DUE TO PROTECTALL SETROPTS PROTECTALL FAILURES is in effect, and the data set has not been protected by a discrete or generic profile.

Exceptions:
• A privileged user bypasses this checking (no auditing done). • A trusted user bypasses the checking, but can be audited with the SETROPTS LOGOPTIONS command. • A user with the SPECIAL attribute gets a warning (see Qualifier 5). • A system-generated temporary data set does not require protection.

5(5)
WARNING ISSUED DUE TO PROTECTALL SETROPTS PROTECTALL WARNING is in effect, and the data set has not been protected by a discrete or generic profile. The authorization request does not fail.

The exceptions in Qualifier 4 also apply.

6(6)
INSUFFICIENT CATEGORY/SECLEVEL The installation uses categories or security levels as separate entities. One of the following occurred:

- The user's SECLEVEL is less than the SECLEVEL of the resource.
- The user is not a member of every CATEGORY associated with the resource.

7(7)
INSUFFICIENT SECURITY LABEL AUTHORITY The SECLABEL class is active and one of the following occurred:

- The user's security label does not dominate the resource's.

- The user does not have a security label, but the resource does.
- SETROPTS MLACTIVE FAILURES is in effect, and either the user or the resource is missing a security label. One exception is explained in Qualifier 8.
- The resource's class requires reverse domination checking, and the resource's security label does not dominate the user's.
- SETROPTS MLS FAILURES is in effect; the user's security label does not equal the resource's, and the requested access is UPDATE or CONTROL. One exception is explained under Qualifier 9.

8(8)
SECURITY LABEL MISSING FROM JOB, USER OR PROFILE One of the following occurred:

- SETROPTS MLACTIVE WARNING is in effect, the SECLABEL class is active, and either the resource or user is missing a security label.
- SETROPTS MLACTIVE FAILURES is in effect, the user has the SPECIAL attribute, and either the resource or the user is missing a security label.

9(9)
WARNING—INSUFFICIENT SECURITY LABEL AUTHORITY One of the following occurred:

- The SECLABEL class is active, SETROPTS MLS WARNING is in effect, the user's security label does not equal the resource's security label, and the requested access is UPDATE or CONTROL.
- SETROPTS MLS FAILURES is in effect, the user's security label does not equal the resource's security label, the requested access is UPDATE or CONTROL, and the user has the SPECIAL attribute.

10(A)
WARNING—DATA SET NOT CATALOGED SETROPTS CATDSNS WARNING is in effect. The data set being accessed cannot be cataloged.

See *z/VM: RACF Security Server Command Language Reference* for more information.

11(B)
DATA SET NOT CATALOGED SETROPTS CATDSNS FAILURES is in effect. The data set being accessed cannot be cataloged. If the user has the SPECIAL attribute, only a warning is issued (see Qualifier 10).

See *z/VM: RACF Security Server Command Language Reference* for more information.

12(C)
PROFILE NOT FOUND—REQUIRED FOR AUTHORITY CHECKING A profile was not found for the general resource, and that resource's class has a default return code greater than 4. The authorization request fails.

13(D)
WARNING—INSUFFICIENT CATEGORY/SECLEVEL The installation uses categories or security levels as separate entities. One of the following occurred:

- The user's SECLEVEL is less than the SECLEVEL of the resource.
- The user is not a member of every CATEGORY associated with the resource.

The resource profile has the WARNING option, so access is given.

Exceptions:
• PROGRAM class profiles cannot use the WARNING option. • RACLISTed profiles can use the WARNING option only if they are RACLISTed by SETROPTS or a RACF 1.8 (or later) RACROUTE REQUEST=LIST.

Event 3(3): ADDVOL/CHGVOL

This event refers to RACROUTE REQUEST=DEFINE,TYPE=ADDVOL and RACROUTE REQUEST=DEFINE,TYPE=CHGVOL.

The explanations of the event code qualifiers for Event 3 are:

0(0)
SUCCESSFUL PROCESSING OF NEW VOLUME One of the following occurred:

- The user has proper administrative authority to the DATASET profile; in the case of tape data sets with TAPEVOL active, the user also had administrative authority to the TAPEVOL profile.
- SETROPTS MLS WARNING is in effect, the TAPEVOL class is active, a TAPEVOL profile exists, and the user's security label does not equal the resource's.
- SETROPTS MLACTIVE WARNING is in effect, the TAPEVOL class is active, and no TAPEVOL profile exists for the volume.

1(1)
INSUFFICIENT AUTHORITY The user did not have administrative authority to the DATASET profile, or, in the case of tape data sets, the TAPEVOL class is active and the user did not have administrative authority to the TAPEVOL profile.

2(2)
INSUFFICIENT SECURITY LABEL AUTHORITY The SECLABEL class is active, the data set is a tape data set, the TAPEVOL class is active, and the user's security label does not dominate the security label found in the TAPEVOL profile.

3(3)
LESS SPECIFIC PROFILE EXISTS WITH DIFFERENT SECLABEL The SECLABEL class is active, SETROPTS MLSTABLE is in effect, a less specific generic profile exists that does not have the same security label, the data set is a tape data set, and the TAPEVOL class is active. Changing the volume would change the TAPEVOL profile's security label, violating SETROPTS MLSTABLE rules.

Exceptions:
If SETROPTS MLQUIET is also in effect and the user has the SPECIAL attribute, the request does not fail and this event is not logged.

Event 4(4): RENAME RESOURCE

This event is based on RACROUTE REQUEST=DEFINE,TYPE=DEFINE,NEWNAME or RACROUTE REQUEST=DEFINE,TYPE=DEFINE,NEWNAMX.

The explanations of the event code qualifiers for Event 4 are:

0(0)
SUCCESSFUL RENAME One of the following occurred:

- The user has sufficient authority to rename the resource.
- The SECLABEL class is active, SETROPTS MLACTIVE WARNING is in effect, and the user or the resource does not have a security label.

1(1)
INVALID GROUP The resource to be renamed is a data set, and the high-level qualifier of the new data set is not a valid group, or user ID.

2(2)
USER NOT IN GROUP The resource is a data set, RACFIND is not set to NO, the high-level qualifier of the new data set name is a group, and the user does not belong to that group.

3(3)
INSUFFICIENT AUTHORITY One of the following occurred:

- SETROPTS GENERICOWNER is in effect, and renaming the profile would violate GENERICOWNER rules.
- The resource is a data set, and the high-level qualifier is a group or user ID. The user is not authorized to create a new data set by the generic profile protecting the new name, and the high-level qualifier of the new data set name is beyond the scope of the user.

- The resource is an SFS file or directory, and the second qualifier is a user ID. The user is not authorized to create a new file or directory by the generic profile protecting the new name, and the second qualifier of the new file or directory name is beyond the scope of the user.

See *z/VM: RACF Security Server Security Administrator's Guide*.

4(4)
RESOURCE NAME ALREADY DEFINED The requested new name already has a discrete profile defined. The return code of the RENAME is 4.

5(5)
USER NOT DEFINED TO RACF The installation's naming convention routine has indicated that the high-level qualifier is a user ID that is not defined to RACF. One of the following occurred:

- RACFIND is not set to NO.
- The resource is protected by a generic or global profile, and the user does not have ALTER access to it.

6(6)
RESOURCE NOT PROTECTED SETROPTS PROTECTALL FAILURES is in effect, and the new data set name is not protected by a profile.

7(7)
WARNING—RESOURCE NOT PROTECTED SETROPTS PROTECTALL WARNINGS is in effect, and the new data set name is not protected by a profile.

The RENAME is allowed.

8(8)
USER IN SECOND QUALIFIER IS NOT RACF DEFINED The second qualifier of the new name is not a valid user ID.

9(9)
LESS SPECIFIC PROFILE EXISTS WITH DIFFERENT SECLABEL The SECLABEL class is active, SETROPTS MLSTABLE is in effect, and there is a less specific generic profile existing for the new name with a different security label. Renaming this resource would violate SETROPTS MLSTABLE rules.

10(A)
INSUFFICIENT SECURITY LABEL AUTHORITY The SECLABEL class is active, SETROPTS MLS FAILURES is in effect, and the user is not authorized to the security label of the resource to be renamed.

11(B)
RESOURCE NOT PROTECTED BY SECURITY LABEL The SECLABEL class is active, SETROPTS MLS FAILURES is in effect, and the profile covering the old resource name does not have a security label.

12(C)
NEW NAME NOT PROTECTED BY SECURITY LABEL The SECLABEL class is active, SETROPTS MLS FAILURES is in effect, and the profile that would cover the new resource name does not have a security label.

13(D)
NEW SECLABEL MUST DOMINATE OLD SECLABEL The SECLABEL class is active, SETROPTS MLS FAILURES is in effect, and the security label of the profile covering the new resource name does not dominate the security label of the profile covering the old resource name.

14(E)
INSUFFICIENT SECURITY LABEL AUTHORITY The SECLABEL class is active, SETROPTS MLS WARNING is in effect, and the user is not authorized to the security label of the profile. The RENAME is allowed.

15(F)
WARNING—RESOURCE NOT PROTECTED BY SECURITY LABEL The SECLABEL class is active, SETROPTS MLS WARNING is in effect, and the profile covering the old resource name does not have a security label. The RENAME is allowed.

16(10)
WARNING—NEW NAME NOT PROTECTED BY SECURITY LABEL The SECLABEL class is active, SETROPTS MLS WARNING is in effect, and the profile that would cover the new resource name does not have a security label. The RENAME is allowed.

17(11)
WARNING—NEW SECLABEL MUST DOMINATE OLD SECLABEL The SECLABEL class is active, SETROPTS MLS WARNING is in effect, and the security label of the profile covering the new resource name does not dominate the security label of the profile covering the old resource name. The RENAME does not fail.

Event 5(5): DELETE RESOURCE

This event is based on RACROUTE REQUEST=DEFINE,TYPE=DELETE.

The explanations of the event code qualifiers for Event 5 are:

0(0)
SUCCESSFUL SCRATCH The resource profile was deleted.

1(1)
RESOURCE NOT FOUND The resource profile was not found.

2(2)
INVALID VOLUME The class is DATASET, and the data set does not reside on the volume specified.

Event 6(6): DELETE ONE VOLUME OF A MULTIVOLUME RESOURCE

This event is based on RACROUTE REQUEST=DEFINE,TYPE=DELETE.

The explanations of the event code qualifiers for Event 6 are:

0(0)
SUCCESSFUL DELETION The volume was successfully deleted from the DATASET profile.

Event 7(7): DEFINE RESOURCE

This event is based on RACROUTE REQUEST=DEFINE,TYPE=DEFINE.

The explanations of the event code qualifiers for Event 7 are:

0(0)
SUCCESSFUL DEFINITION

- The user had sufficient authority to define the resource.
- The SECLABEL class is active, SETROPTS MLACTIVE WARNING is in effect, and the user or the resource does not have a security label.

1(1)
GROUP UNDEFINED The resource to be defined is a data set, and the high-level qualifier is not a valid group or user ID.

2(2)
USER NOT IN GROUP The resource is a data set, RACFIND is not set to NO, the high-level qualifier is a group, and the user does not belong to that group.

3(3)
INSUFFICIENT AUTHORITY One of the following occurred:

- SETROPTS GENERICOWNER is in effect and defining the profile would violate GENERICOWNER rules.
- For general resources, the user is not authorized to define profiles in the class.
- The resource is a data set, and the high-level qualifier of the resource is a group or user ID. The user is not authorized to create a new data set by the generic profile protecting the new name, and the high-level qualifier of the new data set name is beyond the scope of the user.

- The resource is an SFS file or directory, and the second qualifier is a user ID. The user is not authorized to create a new file or directory by the generic profile protecting the new name, and the second qualifier of the new file or directory name is beyond the scope of the user.

See *z/VM: RACF Security Server Security Administrator's Guide*.

4(4)
RESOURCE NAME ALREADY DEFINED The requested name already has a discrete profile defined. The return code of the DEFINE is 4.

5(5)
USER NOT DEFINED TO RACF The installation's naming convention routine has indicated that the high-level qualifier is a user ID that is not defined to RACF. One of the following occurred:

- RACFIND is not set to NO.
- The resource is protected by a generic or global profile, and the user does not have ALTER access to it.

6(6)
RESOURCE NOT PROTECTED SETROPTS PROTECTALL FAILURES is in effect, and the data set to be defined is not protected by a profile.

7(7)
WARNING—RESOURCE NOT PROTECTED SETROPTS PROTECTALL WARNINGS is in effect, and the data set to be defined is not protected by a profile. The DEFINE is allowed.

8(8)
WARNING—SECURITY LABEL MISSING FROM JOB, USER, OR PROFILE The SECLABEL and TAPEVOL classes are active. SETROPTS MLACTIVE WARNING is in effect, and the TAPEVOL profile is without a security label. The DEFINE is allowed.

9(9)
INSUFFICIENT SECURITY LABEL AUTHORITY The SECLABEL and TAPEVOL classes are active. SETROPTS MLS WARNING is in effect, and the user's security label does not dominate the one found in the TAPEVOL profile.

The DEFINE is allowed.

10(A)
USER IN SECOND QUALIFIER IS NOT RACF-DEFINED The second qualifier of the name is not a valid user ID.

11(B)
INSUFFICIENT SECURITY LABEL AUTHORITY The SECLABEL class is active, and one of the following occurred:

- SETROPTS MLACTIVE FAILURES is in effect, and the user is missing a security label.
- SETROPTS MLACTIVE FAILURES is in effect, and the resource is missing a security label.
- The user's security label does not dominate the resource's.
- SETROPTS MLS FAILURES is in effect, and the user's security label does not equal the resource's.

12(C)
LESS SPECIFIC PROFILE EXISTS WITH A DIFFERENT SECLABEL The SECLABEL class is active, SETROPTS MLSTABLE is in effect, and there is a less specific generic profile existing for the name with a different security label.

Defining this resource would violate SETROPTS MLSTABLE rules.

Events 8(8)–25(19): COMMANDS

Events 8 through 25 apply to the RACF commands. The following qualifier codes are used for each event:

0(0)
NO VIOLATIONS DETECTED The RACF command was issued successfully. This qualifier applies to all RACF commands.

1(1)
INSUFFICIENT AUTHORITY The user did not have the authority to issue the RACF command. This qualifier applies to all RACF commands.

2(2)
KEYWORD VIOLATIONS DETECTED The user had the authority to issue the RACF command, but not to all the keywords that were specified. Keywords that the user is not authorized to use are ignored. For example, a user with the SPECIAL attribute but without the AUDITOR attribute can issue the ALTUSER command, but not with the GLOBALAUDIT keyword. This qualifier applies to all RACF commands.

3(3)
SUCCESSFUL LISTING OF DATASETS This logs the successful use of LISTDSD DSNS.

4(4)
SYSTEM ERROR IN LISTING OF DATA SETS This logs an error in attempting LISTDSD DSNS.

Event 26(1A): APPCLU

This event is logged by RACROUTE REQUEST=AUDIT,EVENT='APPCLU'. This event applies to establishing a session between two logical units (referred to as the local LU and the partner LU) in accordance with the System Network Architecture (SNA). VTAM® and CICS® call RACF for security information stored in general resource profiles; the class name is APPCLU.

Each profile contains an 8-byte session key that is used in verification; the two LUs must have corresponding profiles with identical keys so that the handshaking of encrypted data is successful.

The explanations of the event code qualifiers for Event 26 are:

0(0)
PARTNER VERIFICATION WAS SUCCESSFUL The handshaking was successful. The LUs established a connection.

1(1)
SESSION ESTABLISHED WITHOUT VERIFICATION No handshaking was done, but the LUs were still allowed to establish a connection, with the knowledge that the partners were not verified.

2(2)
LOCAL LU KEY WILL EXPIRE IN 5 DAYS OR LESS The handshaking was successful. This qualifier was set to tell users when the local LU's session key would expire.

3(3)
PARTNER LU ACCESS HAS BEEN REVOKED Too many unsuccessful attempts were made at the session key.

4(4)
PARTNER LU KEY DOES NOT MATCH THIS LU KEY An attempt was made, but the session keys did not match; for example, the two sets of identical data encrypted with the two keys did not match.

5(5)
SESSION TERMINATED FOR SECURITY REASONS One or both of the APPCLU profiles involved have the keyword LOCK specified in their session information, preventing any connections from being made. This keyword enables the security administrator to temporarily prevent specific connections without deleting any profiles.

6(6)
REQUIRED SESSION KEY NOT DEFINED The local LU had VERIFY=REQUIRED coded on its APPL statement, indicating that session level verification must be used on all sessions with the LU. One of the following occurred:

- The local LU is the primary LU and no password was defined in RACF for the LU pair.
- The partner LU is the primary LU, but the bind it sent to the local LU did not contain random data (which would indicate that the partner is using session level verification also).

7(7)
POSSIBLE SECURITY ATTACK BY PARTNER LU The local LU sent out a random number to another LU as part of the handshaking process of establishing a session. That same number then came in from a third LU for the local LU to encrypt. It is a coincidence that the same number is chosen; the number is 64 bits of random data.

It may be that an unauthorized user is attempting to steal the encrypted response.

8(8)
SESSION KEY NOT DEFINED FOR PARTNER LU The local LU had VERIFY=OPTIONAL coded on its APPL statement. There was a password defined in the local LU's RACF profile for the LU-LU pair, indicating that session level verification should be used on all sessions between the two LU's. However, the partner LU tried to start a session without using session level verification.

9(9)
SESSION KEY NOT DEFINED FOR THIS LU The local LU had VERIFY=OPTIONAL coded on its APPL statement. No password was defined in the local LU's RACF profile for the LU-LU pair, indicating that session level verification may not be used to establish sessions with this LU. However, the partner LU tried to establish a session using session level verification.

10(A)
SNA SECURITY-RELATED PROTOCOL ERROR The LU trying to establish a connection is not responding correctly according to the handshaking protocol.

11(B)
PROFILE CHANGE DURING VERIFICATION The handshaking was attempted, but it is evident that one of the LU's profiles (specifically the session key) changed in the middle of the handshaking, making its success impossible.

12(C)
EXPIRED SESSION KEY The session key in one or both of the APPCLU profiles has expired.

Event 27(1B): GENERAL AUDITING

This event is logged by RACROUTE REQUEST=AUDIT,EVENT='GENERAL'. RACF does not make any authority checks for this event.

The explanations of the event code qualifiers for Event 27 are:

0 - 99 GENERAL AUDIT RECORD WRITTEN
Qualifiers 0 to 99 can be used for Event 27. These qualifiers are installation defined.

Event 28(IC)–56(38): OPENEXTENSIONS EVENT TYPES

Events 28 through 56 apply to OpenExtensions VM. The following qualifier codes are used for each event:

28(1C)
DIRECTORY SEARCH

0(0)
Access allowed

1(1)
Not authorized to search directory

29(1D)
CHECK ACCESS TO DIRECTORY

0(0)
Access allowed

1(1)
Caller does not have requested access authority

30(1E)
CHECK ACCESS TO FILE

0(0)
Access allowed

1(1)
Caller does not have requested access authority

31(1F)
CHAUDIT

0(0)
File's audit options changed

1(1)
Caller does not have authority to change user audit options of specified file

2(2)
Caller does not have authority to change auditor audit options

33(21)
CHMOD

0(0)
File's mode changed

1(1)
Caller does not have authority to change mode of specified file

34(22)
CHOWN

0(0)
File's owner or group owner changed

1(1)
Caller does not have authority to change owner or group owner of specified file

36(24)
EXEC WITH SETUID/SETGID

0(0)
Successful change of UIDs and GIDs

1(1)
Caller does not have access to the appropriate EXEC.U*uid* profile in the VMPOSIX class.

This qualifier is relevant only to VM.

2(2)
Caller does not have access to the appropriate EXEC.G*gid* profile in the VMPOSIX class.

This qualifier is relevant only to VM.

41(29)
LINK

0(0)
New link created

*****
Failures logged as directory search or check access event types

42(2A)
MKDIR

0(0)
Directory successfully created

*****
Failures logged as directory search or check access event types

43(2B)
MKNOD

0(0)
Successful creation of a node

*****
Failures logged as directory search or check access event types

45(2D)
OPEN (NEW FILE)

0(0)
File successfully created

*****
Failures logged as directory search or check access event types

47(2F)
RENAME

0(0)
Rename successful

*****
Failures logged as directory search or check access event types

48(30)
RMDIR

0(0)
Successful rmdir

*****
Failures logged as directory search or check access event types

49(31)
SETEGID

0(0)
Successful change of effective GID

1(1)
Not authorized to setegid

50(32)
SETEUID

0(0)
Successful change of effective UID

1(1)
Not authorized to seteuid

51(33)
SETGID

0(0)
Successful change of GIDs

1(1)
Not authorized to setgid

52(34)
SETUID

0(0)
Successful change of UIDs

1(1)
Not authorized to setuid

53(35)
SYMLINK

0(0)
Successful symlink

*****
Failures logged as directory search or check access event types

54(36)
UNLINK

0(0)
Successful unlink

*****
Failures logged as directory search or check access event types

56(38)
CHECK FILE OWNER

0(0)
User is the owner

1(1)
User is not the owner

Chapter 4. The Data Security Monitor (DSMON)

RACF enables you to protect resources, but the protection is only as good as the implementation. You need a way to verify that the security mechanisms actually in effect are the ones intended. DSMON helps provide this information for z/VM installations.

DSMON is a program that produces reports on the status of the security environment at your installation and, in particular, on the status of resources that RACF controls. You can use the reports to audit the current status of your installation's system security environment by comparing the actual system characteristics and resource-protection levels with the intended characteristics and levels. You can also control the reporting that DSMON does by specifying control statements that request certain functions for user input.

The DSMON Program

The data security monitor (DSMON) is a program that normally runs while RACF is active.

You must have the AUDITOR or ROAUDIT attribute to run DSMON.

You can specify DSMON control statements to produce the reports you want and control the number of lines per page for each report. The output from DSMON consists of a message data file and output file for the reports.

Note: On both z/OS and z/VM, if you run DSMON while RACF is inactive, DSMON produces only the system report.

1.

How to Run DSMON

The RACDSMON EXEC invokes the DSMON program. RACDSMON produces a CMS file that contains the DSMON control statements used by the DSMON program on z/VM. You can use this file to run the reports or edit the statements in the file to produce the reports you want.

To invoke DSMON on z/VM, you must:

- Have READ access to the RACF service machine's 305 and 490 minidisks and the primary and backup RACF databases
- Have the AUDITOR or ROAUDIT attribute
- IPL the 490 disk
- Access the 305 disk
- Access the CMS 190 disk

Once you are logged on, enter the RACDSMON EXEC:

```
RACDSMON
```

RACF prompts you for the virtual address or addresses of the RACF database or databases.

You can use a CMS subset to access the file RACONFIG EXEC and check the list of addresses for the primary and backup RACF databases at your installation.

Enter the valid virtual address or addresses for your primary database and, if you have one, your backup database. (Be sure to enter the addresses for *all* active RACF databases.)

After you enter the virtual addresses, RACF copies the databases to a temporary disk to enable DSMON to process reports on z/VM. If a file does not already exist, RACDSMON creates a CMS file (ICHDSM00

© Copyright IBM Corp. 1993, 2024

SYSIN) with the following DSMON control statements. You can edit this file by deleting or adding statements to select the type of report you want.

```
FUNCTION SYSTEM
FUNCTION RACGRP
FUNCTION RACCDT
FUNCTION RACEXT
FUNCTION RACGAC
FUNCTION RACUSR
FUNCTION RACDST
```

Specify the DSMON statements you want (including LINECOUNT) or enter FUNCTION ALL to produce all DSMON reports for z/VM. (See "DSMON Control Statements" on page 76 for a description of DSMON control statements.)

Note: If an ICHDSM00 SYSIN file already exists on your A-disk, RACDSMON asks you if you want to overlay the file, use the existing file, or quit. If you use the existing file, RACDSMON produces the reports according to the DSMON statements in the file.

To save your changes and submit the edited file as input to the DSMON program (ICHDSM00), enter the following:

```
FILE
```

The input file that contains the DSMON control statements you have edited (ICHDSM00 SYSIN) is written to your A-disk. The DSMON program uses ICHDSM00 SYSIN to create the reports in an output file and sends the output file and a message file (ICHDSM00 $$$$$$$$) to your virtual printer.

DSMON Control Statements

The three DSMON control statements that allow you to control DSMON reporting are:

- LINECOUNT
- FUNCTION
- USEROPT

On z/VM, you edit the statements contained in the CMS file that RACDSMON produces (see "How to Run DSMON" on page 75).

Entering DSMON Control Statements

DSMON control statements can be entered in any order, one per input line, using columns 1 through 72. You can enter uppercase or lowercase characters. Use commas or blanks to separate list items in each DSMON statement.

You can include comments by entering a /* beginning in column 1. If you want to continue a control statement on a following line, break the statement at any place a blank or comma is allowed and insert a blank followed by a trailing hyphen (-) before you continue to the next line. For example:

```
/* Start of user data sets
USEROPT USRDSN  jim.memo.text vol=8V0L03 -
     jim.report.script
```

The DSMON control statements are:

LINECOUNT number
specifies the number of lines per page for reports. The valid values for number are 0 or a number in the range of 40 through 99. A value of 0 indicates that a page break occurs only at the start of a new report. If you do not specify LINECOUNT, the default is 55 lines per page. If you specify more than one LINECOUNT statement, RACF uses only the last one.

Note: The LINECOUNT statement controls the number of lines per page for the output file. It does not affect the number of lines per page for the SYSPRINT message file (ICHDSM00 $$$$$$$$), fixed at 55 lines per page.

FUNCTION function-name
specifies the DSMON function or functions you want to include.

The default is ALL, which causes DSMON to generate all reports except USRDSN. For a complete description of the DSMON reports specified for function-name, see “Functions DSMON Uses” on page 77.

USEROPT function-name user-input
defines user input to be processed by the function you specify. Function-name specifies the function to process the user-input; user-input specifies the actual input you want processed. The valid functions you can specify for function-name on the USEROPT control statement are:

- RACGRP

Be sure to use one USEROPT control statement for each valid function you want to process the specified input.

USEROPT and RACGRP

Specifying RACGRP with USEROPT causes DSMON to list the group tree and its levels for any specified RACF group name. The following specifies RACGRP for FUNCTION and the RACF group "payroll" (for which all subordinate groups are to be retrieved) for USEROPT RACGRP:

```
FUNCTION RACGRP
USEROPT RACGRP payroll
```

If you specify SYS1 for USEROPT RACGRP, DSMON lists all group names in the system. If you want all DSMON reports but do not specify USEROPT RACGRP, SYS1 is the default group name for the RACF group-tree report. You can, of course, specify any RACF-defined group. For more information on the DSMON report RACGRP produces, see “RACF Group Tree Report” on page 79.

Functions DSMON Uses

DSMON generates different kinds of reports that you can specify on the FUNCTION or USEROPT control statements. After completing each function on the control statement (except for the system report), DSMON issues a message to SYSPRINT stating whether the report executed successfully or unsuccessfully.

If the report ended unsuccessfully, DSMON issues an error code that indicates the cause of the failure. In most cases, DSMON continues processing with the next control statement.

Table 5 on page 77 summarizes the DSMON reports that are generated when you use the FUNCTION control statement. Table 6 on page 78 summarizes the DSMON reports that are generated when you use the USEROPT control statement. You can specify the kind of report you want by modifying function name on each control statement. Both figures list the type of report produced, the system on which the report can be produced, and the information (or checks) each report provides.

Table 5. Reports Specified by the FUNCTION Control Statement

Function-name	Type of Report	Information Provided
SYSTEM	System report	1. Identification number of the processor complex 2. Model number of the processor complex 3. RACF version and release number and whether RACF is active
RACGRP	Group-tree report (also used with USEROPT; Table 6 on page 78)	Group name and level in hierarchy for entire system
RACCDT	RACF class-descriptor table report	All information (see sample report)

Table 5. Reports Specified by the FUNCTION Control Statement (continued)		
Function-name	**Type of Report**	**Information Provided**
RACEXT	RACF exits report	All information (see sample report)
RACGAC	RACF global-access table report	All information (see sample report)
RACUSR	Selected user-attribute report and selected user-attribute summary report	All information (see sample reports)
RACDST	Selected data-sets report	Primary and backup RACF databases

Table 6. Reports Specified by the USEROPT Control Statement		
Function-name	**Type of Report**	**Information Provided**
RACGRP	Group-tree report	Group name and level in hierarchy for user-specified group

DSMON Reports

DSMON produces the following reports:

- System report
- Group-tree report
- RACF class-descriptor table report
- RACF exits report
- RACF global-access-checking table report
- Selected user-attribute report
- Selected user-attribute summary report
- Selected data-sets report
  - Primary and backup RACF databases

Note: Producing the group-tree report or the selected user-attribute report and selected user-attribute summary report can have an impact on system performance. Depending on the size of and load on your RACF databases, you should consider running these DSMON reports during slack time.

The information in the DSMON reports answers many of your audit questions. (See "Conducting the Audit" on page 5.)

System Report

The system report contains the identification number and model of the processor complex and the system identifier (SMF-ID) that SMF uses. The report also specifies the RACF version and release number and whether RACF is active. If RACF is inactive, either because it was not activated at IPL or because it has been deactivated by the RVARY command, DSMON prints a message.

You can use the system report to verify that the system has the expected hardware and software. In addition, you can verify the status of RACF.

Note: DSMON always produces the system report. However, if RACF is not installed and active, DSMON produces only the system report and terminates.

Column Headings

The report contains the following information:

CPU-ID
is the identification number of the processor complex on which the system is running.

CPU MODEL
is the model number of the processor complex.

OPERATING SYSTEM/LEVEL
the name and service level of the z/VM release.

LAST SYSTEM GENERATION
the last time the nucleus was generated.

LAST SYSTEM IPL
the last time an IPL was issued for the nucleus.

Report Messages

The following messages may appear at the end of the report:

RACF VERSION n RELEASE m IS {ACTIVE | INACTIVE | HAS BEEN DEACTIVATED}

Explanation

- If "ACTIVE" appears in the message text, the specified version of RACF is active. In most cases, this is the message that appears on the report. If the version and release specified is a level of RACF earlier than Version 1 Release 8, DSMON produces a separate error message stating that the version is unknown and the program terminates.
- If "INACTIVE" appears in the message text, the specified version of RACF was not activated during initial program load (IPL). Under normal circumstances, this message should not appear. If it does, notify your RACF security administrator or your installation manager.
- If "HAS BEEN DEACTIVATED" appears in the message text, the specified version of RACF has been deactivated by the RVARY command; this situation is normally temporary.

RACF IS NOT INSTALLED

Explanation

DSMON cannot locate the RACF communications vector table (RCVT), indicating that RACF has not been installed.

Note: Under normal circumstances, this message should not appear. If it does, notify your RACF security administrator or your installation manager.

RACF VERSION UNKNOWN

Explanation

DSMON retrieved a RACF version and release number from the RCVT, but they identify a level of RACF that is earlier than RACF Version 1 Release 8.

Note: Under normal circumstances, this message should not appear. If it does, notify your RACF security administrator or your installation manager.

Sample System Report

```
                                    S Y S T E M     R E P O R T
-------------------------------------------------------------------------------------------------------------------
CPU-ID                          319B9E
CPU MODEL                       2094
OPERATING SYSTEM/LEVEL          z/VM Version 5 Release 3.0, service level 0000
LAST SYSTEM GENERATION          Generated at 12/08/06 11:06:55 EST
LAST SYSTEM IPL                 IPL at 01/02/07 18:49:24 EST
RACF VERSION 5 RELEASE 3 IS ACTIVE
```

Figure 15. Sample System Report (z/VM)

RACF Group Tree Report

The group-tree report lists all subgroups for the SYS1 group and continues to list subgroups for those subgroups on down the group tree. Alternately, if a user-specified group name is specified for the USEROPT control statement, the report lists all subgroups for that user-supplied group. The report provides the owner's name for each group, if the owner is not the superior group.

You can use the group-tree report to examine the overall RACF group structure for your system. You can also determine how the group-related attributes (group-SPECIAL, group-OPERATIONS, and group-AUDITOR) for users associated with each subgroup are related. In this way, you can decide whether the group authorities are structured effectively for your system.

Column Headings

LEVEL
Starting with the highest requested group, the group-level number that indicates the relative nesting level of the group or subgroup within the requested group tree. SYS1 is always 1; the groups with SYS1 as their superior group are 2, and so on down the group tree.

GROUP
is the name of the RACF-defined group.

(OWNER)
is the name of the owner of the group. This name is listed only if the owner is not the superior group.

Report Messages

An arrow (===>) in the report indicates that the information has overflowed the right margin. The missing information appears after the main body of the report is printed. The characters -----CONTINUATION----- appear before the overflowed information, and the discontinued level number, group, and owner name (if the name is not the same as that of the superior group) appear in the left margin.

```
                                R A C F    G R O U P    T R E E    R E P O R T
LEVEL   GROUP      (OWNER)
-------------------------------------------------------------------------------------------------------------------

    1   SYS1       (IBMUSER )
    2   | ALL        (IBMUSER )
    2   | C49TEST    (IBMUSER )
    2   | INFO       (IBMUSER )
    2   | JESS       (IBMUSER )
    2   | LIBS       (IBMUSER )
    2   | MASTER     (IBMUSER )
    2   | OPERCNTL   (IBMUSER )
    2   | OPERRD     (IBMUSER )
    2   | OPERUP     (IBMUSER )
    2   | SYSCTLG    (IBMUSER )
    2   | SYS3       (IBMUSER )
    2   | VSAMDSET   (IBMUSER )
```

Figure 16. Sample Group-Tree Report

RACF Class-Descriptor Table Report

The class-descriptor table report lists class name and status for all general resource classes in the class-descriptor table, as well as information about auditing activity, statistics, the activity of OPERATIONS users, and the universal access authority (UACC).

You can use the class-descriptor table report to determine the resource classes defined to RACF for your system. In this way, you can obtain information about the protection status of any resource in the class-descriptor table.

Column Headings

CLASS NAME
is the class name found in the RACF class-descriptor table.

STATUS
indicates whether the class is active or inactive.

AUDITING
indicates whether there is auditing for the class. The value is either YES or NO.

STATISTICS
indicates whether RACF is gathering statistics for the class. The value is either YES or NO.

DEFAULT UACC
indicates the default UACC defined for the class in the class-descriptor table. RACF uses this UACC for profiles defined to the class, unless the UACC operand is specified on the RDEFINE command that writes the profile.

The following values may appear:

- ALTER
  - For discrete profiles, ALTER indicates that, by default, all users have control over the resource and the resource profile and can authorize other users or groups (or both) to access the resource.
  - For generic profiles, ALTER indicates that, by default, all users have control over the resource and can allocate data sets protected by the generic profile. Only the profile owner has full control over the resource profile.
- CONTROL indicates that, by default, all users have access authority to update, insert, or delete records in the VSAM data set and perform other operations as if the data-set password were supplied.
- UPDATE indicates that, by default, all users can access the resource for both reading and writing.
- READ indicates that, by default, all users can access the resource for reading only.
- NONE indicates that, by default, users cannot access the resource.
- ACEE indicates that the UACC is taken from the accessor-environment element (ACEE).

OPERATIONS
indicates whether RACF is to use the OPERATIONS attribute authority during authorization checking. A value of YES indicates RACF performs authorization checking; a value of NO indicates it does not.

Report Messages

The following message may appear below the report column headings:

NO ENTRIES	**IN THE RACF CLASS DESCRIPTOR TABLE**

Explanation

There are no entries in the class-descriptor table. RACF includes a basic class descriptor table, required for RACF processing. If you receive this message, report the condition to your RACF security administrator or installation manager.

Sample RACF Class-Descriptor Table Report

```
                        R A C F    C L A S S    D E S C R I P T O R    T A B L E    R E P O R T

CLASS                                                                  DEFAULT       OPERATIONS
NAME           STATUS        AUDITING        STATISTICS              UACC          ALLOWED
-------------------------------------------------------------------------------------------------------------------
----------
RVARSMBR       ACTIVE          NO                NO                  NONE            NO
RACFVARS       ACTIVE          NO                NO                  NONE            NO
SECLABEL       INACTIVE        NO                NO                  NONE            NO
VMMDISK        ACTIVE          NO                NO                  NONE            YES
VMRDR          ACTIVE          NO                NO                  NONE            YES
VMCMD          ACTIVE          NO                NO                  NONE            YES
VMNODE         ACTIVE          NO                NO                  NONE            YES
VMBATCH        ACTIVE          NO                NO                  NONE            YES
FILE           ACTIVE          YES               NO                  NONE            YES
DIRECTRY       ACTIVE          YES               NO                  NONE            YES
SFSCMD         ACTIVE          NO                NO                  NONE            NO
VMPOSIX        ACTIVE          NO                NO                  NONE            NO
VMMAC          INACTIVE        NO                NO                  NONE            NO
VMSEGMT        INACTIVE        NO                NO                  NONE            NO
DIRSRCH        ACTIVE          NO                NO                  NONE            NO
DIRACC         ACTIVE          NO                NO                  NONE            NO
FSOBJ          ACTIVE          NO                NO                  NONE            NO
FSSEC          ACTIVE          NO                NO                  NONE            NO
PROCESS        INACTIVE        NO                NO                  NONE            NO
DASDVOL        INACTIVE        NO                NO                  ACEE            YES
GDASDVOL       INACTIVE        NO                NO                  ACEE            YES
TAPEVOL        INACTIVE        NO                NO                  ACEE            YES
TERMINAL       ACTIVE          NO                NO                  ACEE            NO
GTERMINL       ACTIVE          NO                NO                  ACEE            NO
APPL           INACTIVE        NO                NO                  NONE            NO
TIMS           INACTIVE        NO                NO                  NONE            NO
GIMS           INACTIVE        NO                NO                  NONE            NO
AIMS           INACTIVE        NO                NO                  NONE            NO
TCICSTRN       INACTIVE        NO                NO                  NONE            NO
GCICSTRN       INACTIVE        NO                NO                  NONE            NO
PCICSPSB       INACTIVE        NO                NO                  NONE            NO
QCICSPSB       INACTIVE        NO                NO                  NONE            NO
GLOBAL         INACTIVE        NO                NO                  NONE            NO
GMBR           INACTIVE        NO                NO                  NONE            NO
DSNR           INACTIVE        NO                NO                  ACEE            NO
FACILITY       ACTIVE          NO                NO                  NONE            NO
SCDMBR         INACTIVE        NO                NO                  NONE            NO
SECDATA        INACTIVE        NO                NO                  NONE            NO
FCICSFCT       INACTIVE        NO                NO                  NONE            NO
HCICSFCT       INACTIVE        NO                NO                  NONE            NO
JCICSJCT       INACTIVE        NO                NO                  NONE            NO
KCICSJCT       INACTIVE        NO                NO                  NONE            NO
DCICSDCT       INACTIVE        NO                NO                  NONE            NO
ECICSDCT       INACTIVE        NO                NO                  NONE            NO
SCICSTST       INACTIVE        NO                NO                  NONE            NO
UCICSTST       INACTIVE        NO                NO                  NONE            NO
MCICSPPT       INACTIVE        NO                NO                  NONE            NO
NCICSPPT       INACTIVE        NO                NO                  NONE            NO
ACICSPCT       INACTIVE        NO                NO                  NONE            NO
BCICSPCT       INACTIVE        NO                NO                  NONE            NO
PMBR           ACTIVE          NO                NO                  NONE            NO
PROGRAM        ACTIVE          NO                NO                  NONE            NO
TSOPROC        INACTIVE        NO                NO                  NONE            NO
ACCTNUM        INACTIVE        NO                NO                  NONE            NO
PERFGRP        INACTIVE        NO                NO                  NONE            NO
TSOAUTH        INACTIVE        NO                NO                  NONE            NO
MGMTCLAS       INACTIVE        NO                NO                  NONE            NO
STORCLAS       INACTIVE        NO                NO                  NONE            NO
FIELD          INACTIVE        NO                NO                  NONE            NO
```

Figure 17. Class-Descriptor Table Report (Part 1 of 2)

```
                        R A C F    C L A S S    D E S C R I P T O R    T A B L E    R E P O R T

CLASS                                                                  DEFAULT       OPERATIONS
NAME           STATUS        AUDITING        STATISTICS              UACC          ALLOWED
-------------------------------------------------------------------------------------------------------------
----------
CCICSCMD       INACTIVE        NO               NO                    NONE            NO
VCICSCMD       INACTIVE        NO               NO                    NONE            NO
VMBR           INACTIVE        NO               NO                    NONE            NO
VMEVENT        INACTIVE        NO               NO                    NONE            NO
PROPCNTL       INACTIVE        NO               NO                    NONE            NO
APPCLU         INACTIVE        NO               NO                    NONE            NO
SMESSAGE       INACTIVE        NO               NO                    NONE            NO
DEVICES        INACTIVE        NO               NO                    NONE            NO
VTAMAPPL       INACTIVE        NO               NO                    NONE            NO
PSFMPL         INACTIVE        NO               NO                    NONE            YES
OPERCMDS       INACTIVE        NO               NO                    NONE            NO
WRITER         INACTIVE        NO               NO                    NONE            NO
JESSPOOL       INACTIVE        NO               NO                    NONE            NO
JESJOBS        INACTIVE        NO               NO                    NONE            NO
JESINPUT       INACTIVE        NO               NO                    NONE            NO
CONSOLE        INACTIVE        NO               NO                    NONE            NO
TEMPDSN        INACTIVE        NO               NO                    NONE            NO
DIRAUTH        INACTIVE        NO               NO                    NONE            NO
SURROGAT       ACTIVE          NO               NO                    NONE            NO
NODMBR         INACTIVE        NO               NO                    NONE            NO
NODES          INACTIVE        NO               NO                    NONE            NO
PIMS           INACTIVE        NO               NO                    NONE            NO
QIMS           INACTIVE        NO               NO                    NONE            NO
SIMS           INACTIVE        NO               NO                    NONE            NO
UIMS           INACTIVE        NO               NO                    NONE            NO
FIMS           INACTIVE        NO               NO                    NONE            NO
HIMS           INACTIVE        NO               NO                    NONE            NO
OIMS           INACTIVE        NO               NO                    NONE            NO
WIMS           INACTIVE        NO               NO                    NONE            NO
NVASAPDT       INACTIVE        NO               NO                    NONE            NO
VXMBR          ACTIVE          NO               NO                    NONE            NO
VMXEVENT       ACTIVE          NO               NO                    NONE            NO
CIMS           INACTIVE        NO               NO                    NONE            NO
DIMS           INACTIVE        NO               NO                    NONE            NO
DLFCLASS       INACTIVE        NO               NO                    NONE            NO
SDSF           INACTIVE        NO               NO                    NONE            NO
GSDSF          INACTIVE        NO               NO                    NONE            NO
CSFSERV        INACTIVE        NO               NO                    NONE            NO
CSFKEYS        INACTIVE        NO               NO                    NONE            NO
GCSFKEYS       INACTIVE        NO               NO                    NONE            NO
APPCTP         INACTIVE        NO               NO                    NONE            NO
APPCSI         INACTIVE        NO               NO                    READ            NO
APPCPORT       INACTIVE        NO               NO                    NONE            NO
RMTOPS         INACTIVE        NO               NO                    NONE            NO
INFOMAN        INACTIVE        NO               NO                    ACEE            NO
GINFOMAN       INACTIVE        NO               NO                    ACEE            NO
APPCSERV       INACTIVE        NO               NO                    NONE            NO
PTKTDATA       INACTIVE        NO               NO                    NONE            NO
LFSCLASS       INACTIVE        NO               NO                    NONE            NO
RODMMGR        INACTIVE        NO               NO                    ACEE            YES
MQQUEUE        INACTIVE        NO               NO                    NONE            NO
GMQQUEUE       INACTIVE        NO               NO                    NONE            NO
MQPROC         INACTIVE        NO               NO                    NONE            NO
GMQPROC        INACTIVE        NO               NO                    NONE            NO
MQNLIST        INACTIVE        NO               NO                    NONE            NO
GMQNLIST       INACTIVE        NO               NO                    NONE            NO
MQADMIN        INACTIVE        NO               NO                    NONE            NO
GMQADMIN       INACTIVE        NO               NO                    NONE            NO
MQCMDS         INACTIVE        NO               NO                    NONE            NO
MQCONN         INACTIVE        NO               NO                    NONE            NO
```

Figure 18. Class-Descriptor Table Report (Part 2 of 2)

RACF Exits Report

The RACF exits report lists the names of all the installation-defined RACF exit routines and specifies the size of each exit-routine module. DSMON prints an error message if the RACF communications vector table (RCVT), which contains the address of each RACF exit routine module, indicates that an exit-routine module should exist but the module cannot be loaded, or the entry address does not correspond with the address specified in the RCVT.

You can use this report to verify that the only active exit routines are those that your installation has defined. The existence of any other exit routines may indicate a system security exposure, because RACF exit routines could be used to bypass RACF security checking. Similarly, if the length of an exit-

routine module differs from the length of the module your installation defined, the module may have unauthorized modifications.

Column Headings

EXIT MODULE NAME
is the name of the RACF exit routine module, as defined by your installation.

MODULE LENGTH
is the length of the exit routine module in bytes (decimal).

Report Messages

The following message may appear below the report column headings:

NO RACF EXITS ARE ACTIVE

Explanation

There are no active RACF exit routines. This absence does not indicate an abnormal condition, unless your installation has defined RACF exit routines.

Sample RACF Exits Report

```
                                                R A C F    E X I T S    R E P O R T

EXIT MODULE          MODULE
NAME                 LENGTH
-------------------------------------------------------------------------------------------------------------------
NO RACF EXITS ARE ACTIVE
```

Figure 19. Sample RACF Exits Report

RACF Global Access-Checking Table Report

The global access-checking table report lists all entries in the global access-checking table. Each entry consists of a resource name and its associated global access-checking authority level.

Also, you can use the global access-checking table report to determine whether protection for a sensitive resource is adequate. By examining the global access information for an entry, you can discover whether the global access authority level provides the right security for the resource.

Column Headings

CLASS NAME
is the class name found in the global access checking table.

ENTRY NAME
is the entry name or names defined in each class. If the GLOBAL class is inactive, GLOBAL INACTIVE appears in this column. If the GLOBAL class is active but no members are defined for the class, NO ENTRIES appears in the column.

ACCESS LEVEL
specifies the global access checking authority level for the entry.

Report Messages

The following message may appear below the report column headings:

GLOBAL INACTIVE

Explanation

There are no entries in the RACF global access checking table. This message does not indicate an error condition. When RACF is initially installed, for example, the RACF global access checking table normally contains no entries.

Sample RACF Global Access-Checking Table Report

```
                              R A C F    G L O B A L    A C C E S S    T A B L E    R E P O R T
CLASS           ACCESS          ENTRY
NAME            LEVEL           NAME
-------------------------------------------------------------------------------------------------------------
----------
DATASET         READ            IBMUSER.GENERIC.*
                READ            ISPF.*
                READ            LAURIE.ALL.CAN.READ.THIS.DATASET
                UPDATE          SYS1.BRODCAST
                READ            &RACGPID;*
                ALTER           &RACUID;*
RVARSMBR                        -- NO ENTRIES --
SECLABEL                        -- NO ENTRIES --
DASDVOL                         -- NO ENTRIES --
TAPEVOL                         -- NO ENTRIES --
TERMINAL                        -- NO ENTRIES --
APPL                            -- NO ENTRIES --
TIMS                            -- NO ENTRIES --
AIMS                            -- NO ENTRIES --
TCICSTRN                        -- NO ENTRIES --
PCICSPSB                        -- NO ENTRIES --
GMBR                            -- NO ENTRIES --
DSNR                            -- NO ENTRIES --
FACILITY                        -- NO ENTRIES --
VMMDISK         READ            MAINT.190
                ALTER           &RACUID;190
VMRDR                           -- NO ENTRIES --
VMCMD                           -- NO ENTRIES --
VMNODE                          -- NO ENTRIES --
VMBATCH                         -- NO ENTRIES --
SCDMBR                          -- NO ENTRIES --
FCICSFCT                        -- NO ENTRIES --
JCICSJCT                        -- NO ENTRIES --
DCICSDCT                        -- NO ENTRIES --
SCICSTST                        -- NO ENTRIES --
MCICSPPT                        -- NO ENTRIES --
ACICSPCT                        -- NO ENTRIES --
PMBR                            -- NO ENTRIES --
TSOPROC                         -- NO ENTRIES --
ACCTNUM                         -- NO ENTRIES --
PERFGRP                         -- NO ENTRIES --
TSOAUTH                         -- NO ENTRIES --
MGMTCLAS                        -- NO ENTRIES --
STORCLAS                        -- NO ENTRIES --
FIELD                           -- NO ENTRIES --
CCICSCMD                        -- NO ENTRIES --
PROPCNTL                        -- NO ENTRIES --
APPCLU                          -- NO ENTRIES --
SMESSAGE                        -- NO ENTRIES --
DEVICES                         -- NO ENTRIES --
VTAMAPPL                        -- NO ENTRIES --
PSFMPL                          -- NO ENTRIES --
```

Figure 20. Sample RACF Global Access-Checking Table Report (Part 1 of 2)

```
                                R A C F    G L O B A L    A C C E S S    T A B L E    R E P O R T
CLASS            ACCESS           ENTRY
NAME             LEVEL            NAME
-------------------------------------------------------------------------------------------------------------
----------
OPERCMDS                          -- NO ENTRIES --
WRITER                            -- NO ENTRIES --
JESSPOOL                          -- NO ENTRIES --
JESJOBS                           -- NO ENTRIES --
JESINPUT                          -- NO ENTRIES --
CONSOLE                           -- NO ENTRIES --
TEMPDSN                           -- NO ENTRIES --
DIRAUTH                           -- NO ENTRIES --
SURROGAT                          -- NO ENTRIES --
NODMBR                            -- NO ENTRIES --
NODES                             -- NO ENTRIES --
PIMS                              -- NO ENTRIES --
SIMS                              -- NO ENTRIES --
FIMS                              -- NO ENTRIES --
OIMS                              -- NO ENTRIES --
NVASAPDT                          -- NO ENTRIES --
VXMBR                             -- NO ENTRIES --
DIRECTRY    READ                  POOL1.PROFS.GENERALINFO.*
            READ                  POOL1.MAINT.CPHELP.**
            READ                  POOL1.TOOLS.IBMVM.**
FILE        UPDATE                POOL1.PROFS.GENERALINFO.*.USER.TALK
            READ                  POOL1.MAINT.CPHELP.**.*.HELP*
            UPDATE                POOL1.TOOLS.IBMVM.**.*.FORUM
CIMS                              -- NO ENTRIES --
DLFCLASS                          -- NO ENTRIES --
SFSCMD                            -- NO ENTRIES --
SDSF                              -- NO ENTRIES --
```

Figure 21. Sample RACF Global Access-Checking Table Report (Part 2 of 2)

Selected User-Attribute Report

The selected user-attribute report lists all RACF users with the SPECIAL, OPERATIONS, AUDITOR, ROAUDIT, or REVOKE attribute and indicates whether a user possesses the attribute on a system (user) or group level.

You can use the selected user-attribute report to verify that only those users who need to be authorized to perform certain functions have been assigned the corresponding attribute.

Column Headings

USERID
is the user's system identifier.

ATTRIBUTE TYPE
identifies each attribute and indicates whether the user has the attribute on a system (user) or a group level. SYSTEM indicates the user has that attribute on a system level, or at all times. GROUP indicates user has the attribute only within one or more of the groups to which the user is connected. If neither SYSTEM nor GROUP appears, the user does not possess that attribute on either level.

If a user has one or more attributes on a group level, you can determine the names of the corresponding group or groups through the LISTUSER command or the "User Services" panel.

The report lists the following attribute types:

SPECIAL
gives the user complete control over all the RACF profiles in the RACF database and authority to issue all RACF commands, except those reserved for the auditor's use.

OPERATIONS
gives the user authority to perform maintenance operations and provides full authority to access RACF-protected DASD data sets and certain resource classes.

AUDITOR
gives the user complete authority to audit security controls and the use of system resources.

ROAUDIT
gives the user authority to audit the use of system resources.

REVOKE
prevents, on a system level, a RACF-defined user from entering the system at all. On a group level, a user can enter the system but cannot use any group authorities associated with the group, or access data sets using that group's authority.

Note: When REVOKE is specified with a future date, the status change does not occur until the specified date. Until that date, the report does not list the user as revoked.

For more information on each attribute, especially at the group level, see *z/VM: RACF Security Server Security Administrator's Guide*.

Report Messages

The following message may appear below the report column headings:

NO SELECTED	**USERS FOUND**

Explanation

There are no users with the SPECIAL, OPERATIONS, AUDITOR, ROAUDIT, or REVOKE attributes on either a system or group level.

Note: Under normal circumstances, this message should not appear. At least one user should have the SPECIAL attribute on a system level, and at least one user should have the AUDITOR or ROAUDIT attribute on a system level. If this message appears, notify your RACF security administrator or your installation manager.

Sample Selected User-Attribute Report

```
                              S E L E C T E D    U S E R    A T T R I B U T E    R E P O R T
USERID           ----------------  ATTRIBUTE TYPE  ---------------
                 SPECIAL        OPERATIONS     AUDITOR        ROAUDIT        REVOKE
-------------------------------------------------------------------------------------------------------
----------
GENSTP           SYSTEM
IBMUSER          SYSTEM         SYSTEM         SYSTEM
JESA             SYSTEM
JESB             SYSTEM
JESC             SYSTEM
JESD             SYSTEM
JESE             SYSTEM
JESF             SYSTEM
JESID            SYSTEM
JES2             SYSTEM
JES3             SYSTEM
JES3CI           SYSTEM
JES4             SYSTEM
JES5             SYSTEM
JES6             SYSTEM
JES7             SYSTEM
JES8             SYSTEM
JES9             SYSTEM
OPER24           GROUP
OPER25           GROUP
PSF              SYSTEM
SPL0             SYSTEM
SPL1             SYSTEM
SPL10            SYSTEM
SPL11            SYSTEM
SPL12            SYSTEM
SPL13            SYSTEM
SPL14            SYSTEM
SPL15            SYSTEM
SPL16            SYSTEM
SPL17            SYSTEM
SPL19            SYSTEM
SPL2             SYSTEM
SPL20            SYSTEM
SPL21            SYSTEM
SPL22            SYSTEM
SPL23            SYSTEM
SPL24            SYSTEM
SPL3             SYSTEM
SPL4             SYSTEM
SPL5             SYSTEM
SPL6             SYSTEM
SPL7             SYSTEM
SPL7A            SYSTEM                        SYSTEM
SPL8             SYSTEM
SPL9             SYSTEM
SUPERU           SYSTEM                        SYSTEM
VTAM             SYSTEM
```

Figure 22. Sample Selected User-Attribute Report

Sample Selected User-Attribute Summary Report

The selected user-attribute summary report shows totals for installation-defined users and for users with the SPECIAL, OPERATIONS, AUDITOR, ROAUDIT, and REVOKE attribute at both the system and the group level. You can use the summary report to verify that the number of users with each of the selected attributes, on either a system or a group level, is the number your installation wants.

Note: The selected user-attribute summary report is produced automatically after the selected user-attribute report; it cannot be requested separately.

Column Headings

TOTAL DEFINED USERS
is the number of users defined by your installation.

TOTAL SELECTED ATTRIBUTE USERS
is the number of users with each of the selected attributes (SPECIAL, OPERATIONS, AUDITOR, ROAUDIT, and REVOKE) at both the system and group level.

Report Messages

No messages appear at the end of this report.

```
S E L E C T E D    U S E R    A T T R I B U T E    S U M M A R Y    R E P O R T
-------------------------------------------------------------------------------------------------------------------
TOTAL DEFINED USERS:         448
TOTAL SELECTED ATTRIBUTE USERS:
ATTRIBUTE BASIS          SPECIAL      OPERATIONS         AUDITOR          ROAUDIT          REVOKE
---------------          -------      ----------         -------          -------          ------
SYSTEM                        47               1               3                0               0
GROUP                          2               0               0                0               0
```

Figure 23. Selected User-Attribute Summary Report

Selected Data-Sets Report

The selected data-sets report lists all the data sets, including the RACF database or databases, that meet one or more of the selection criteria that DSMON uses. For each selected data set, the report specifies the serial number of the volume on which the data set resides, the selection criterion, whether the data set is RACF-indicated or RACF-protected, and the universal access authority (UACC) for the data set. If a data set or RACF database meets more than one selection criterion, there is a separate entry for each criterion.

On z/VM, you can use the selected data-sets report to obtain information about primary and backup databases.

Column Headings

DATA SET NAME
is the name of the data set.

VOLUME SERIAL
is the serial number of the direct access volume on which the data set resides. If the data set is not cataloged, this column is blank.

SELECTION CRITERION
is the criterion that was used to select the data set for the report.

The following entries may appear:

RACF PRIMARY
means the data set is a primary RACF database, containing RACF access-control information. This information includes user, group, connect, data-set, and general-resource profiles.

RACF BACKUP
means the data set is a backup or recovery RACF database.

RACF INDICATED
indicates whether the data set is RACF-indicated.

The following entries may appear:

YES
means the RACF indicator for the data set is on.

NO
means the RACF indicator for the data set is off.

RACF PROTECTED
indicates whether the data set has a RACF profile. The following entries may appear:

YES
means the data set has a discrete or generic profile. If the RACF indicator for the data set is on, the data set is protected by a discrete profile.

NO
means no profile exists for the data set. The data set is not protected in any way by RACF.

Note: On z/VM, this column will show that the RACF databases are not protected, as DATASET profiles do not protect the RACF databases in the z/VM environment. On z/VM you should validate the protection of the RACF databases by ensuring that the minidisks that the RACF databases reside on are protected by a profile in the VMMDISK class.

UACC
is the data set's universal access authority (UACC), if it is defined. The UACC is the default access authority that specifies how the data set can be accessed by users or groups not in the access list of the data set's RACF profile.

Note:

1. The UACC does not necessarily indicate the actual authority that a user has to access the data set. The global access-checking table may contain an entry applicable to the data set, or the user may be on the access list, if the data set has a discrete profile.
2. On z/VM, this column will be blank.

The following universal access authorities may appear:

ALTER
For a data set that is protected by a discrete profile, ALTER allows all users to read, update, or delete the data set.

CONTROL
For VSAM (virtual storage access method) data sets, CONTROL provides all users with the same authority that is provided with the VSAM CONTROL password; that is, authority to perform control-interval access (access to individual VSAM data blocks), and to retrieve, update, insert, or delete records in the specified data set.

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

UPDATE
allows all users to read or update the data set. UPDATE does not, however, authorize a user to delete the data set.

READ
allows all users to access the data set for reading or copying only.

NONE
does not allow users to access the data set.

Report Messages

The following message may appear below the report column headings:

NO SELECTED DATA SETS FOUND

Explanation

DSMON did not find any data sets meeting the criteria.

Note: Under normal circumstances, this message should not appear. If it does, notify your RACF security administrator or installation manager.

Sample Selected Data-Sets Report

```
                                  S E L E C T E D    D A T A    S E T S    R E P O R
T
                                            VOLUME     SELECTION          RACF
RACF
DATA SET NAME                               SERIAL     CRITERION          INDICATED       PROTECTED
UACC
-------------------------------------------------------------------------------------------------------------------
RACF.BACKUP                                 RACFBK     RACF BACKUP        YES
NO
RACF.DATASET                                RACF       RACF PRIMARY       YES             NO
```

Figure 24. Sample Selected Data-Sets Report

Appendix A. The RACF Report Writer

Attention:
The report writer is no longer the IBM-recommended utility for processing RACF audit records. The RACF SMF data unload utility is the preferred reporting utility. The report writer does not support many of the audit records introduced after RACF 1.9.2. Refer to Chapter 3, “RACF SMF Data Unload Utility (RACFADU),” on page 49 for more details.

A successful security mechanism requires that appropriate personnel, particularly the auditor and the security administrator, be able to assess the implementation of the security mechanism and the use of the resources it protects. The RACF report writer provides a wide range of reports that enable you to monitor and verify the use of the system and resources.

The RACF report writer lists the contents of System Management Facilities (SMF) records in a format that is easy to read. SMF records reside in the SMF data file. You can also tailor the reports to select specific SMF records that contain certain kinds of RACF information. With the RACF report writer, you can obtain:

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

How the RACF Report Writer Operates

The RACF report writer consists of three phases:

- Command and subcommand processing
- Record selection
- Report generation.

See Figure 25 on page 92 for an overview of the RACF report writer. Figure 25 on page 92 also shows the replaceable module, ICHRSMFI, for the RACF report writer, and the RACF report writer installation-wide exit, ICHRSMFE.

ICHRSMFI is a nonexecutable module that contains default values for the RACF report writer sort parameters, dynamic allocation parameters, and processing options. See *z/VM: RACF Security Server System Programmer's Guide* for a description of the contents of the module and an explanation of how to modify the module if necessary.

ICHRSMFE is an installation-wide exit that the RACF report writer calls during the record selection phase. The exit allows you to add functions such as the following to the RACF report writer:

- Create additional selection and or rejection criteria (or both) for records that the RACF report writer processes
- For z/OS data sets, modify naming conventions in records that the RACF report writer processes
- Add other reports to those that the RACF report writer provides

Detailed information about coding the ICHRSMFE exit routine appears in *z/VM: RACF Security Server System Programmer's Guide*.

© Copyright IBM Corp. 1993, 2024

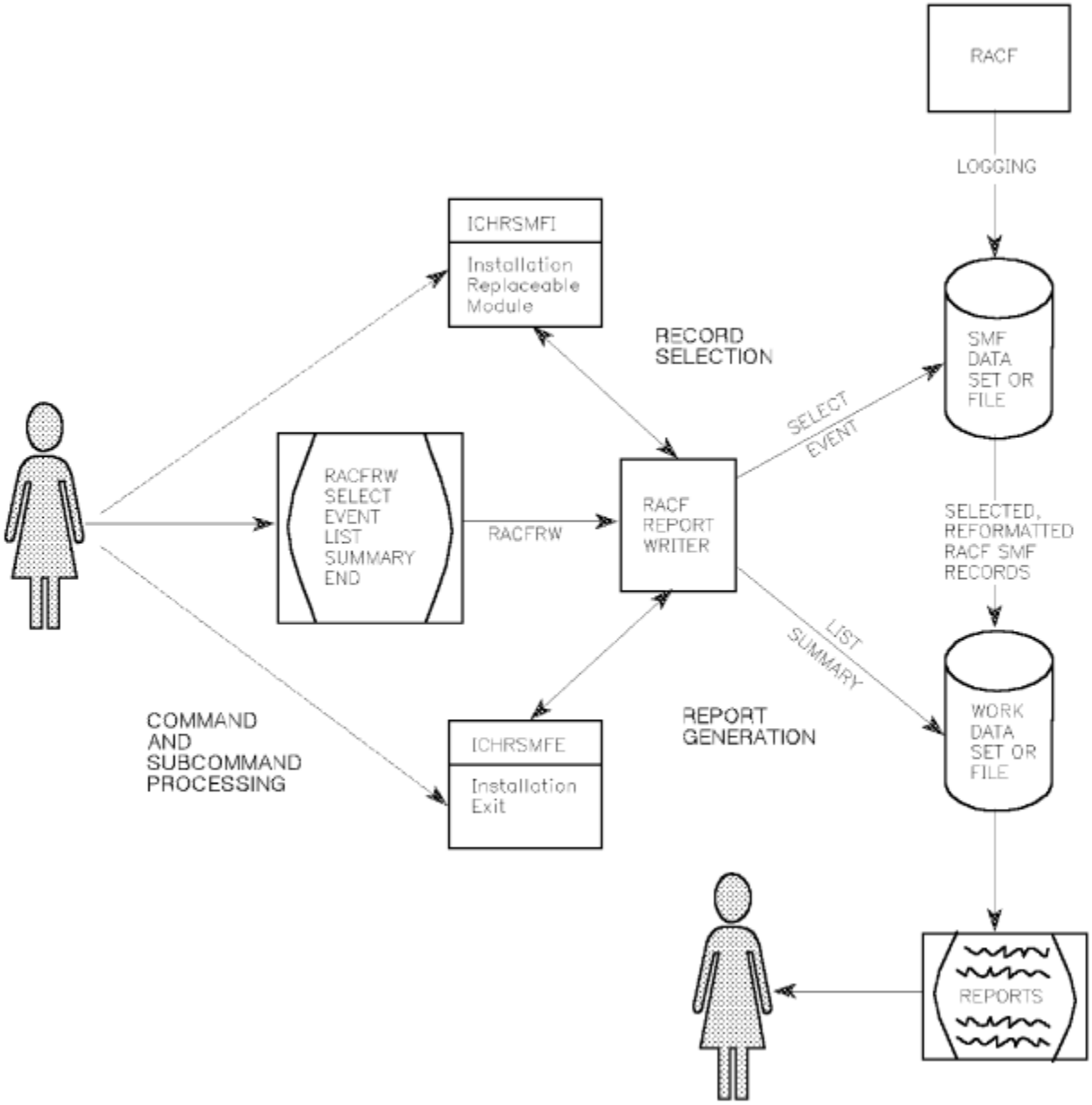

Figure 25. RACF Report Writer Overview

Phase 1

Command and Subcommand Processing:

Command and subcommand processing start when you invoke the RACRPORT EXEC. To execute RACRPORT EXEC while RACF is active, you need a user ID with read access to the RACF service machine's 191, 301, 302, 305, and 490 minidisks. Execute the RACRPORT EXEC from that user ID. You must IPL the 490 minidisk before issuing the RACRPORT EXEC. Initially, you must ensure that you are linked to the appropriate minidisks, including the SMF minidisk. The commands used by RACRPORT (the RACFRW command and the SELECT, EVENT, LIST, SUMMARY, and END subcommands) must be placed in a file called RACFRW CONTROL on your A-disk.

Briefly, the SELECT and EVENT subcommands specify which of the input records the RACF report writer selects and uses to generate the reports. You can then produce those reports by using the LIST

subcommand to format and print a listing of each SMF record you select and the SUMMARY subcommand to format and print a summary listing of the SMF records. After entering all the subcommands you need, enter the END subcommand. END terminates subcommand mode and the first processing phase.

Note: Pressing PA1 or the attention key at any time during this first phase terminates the RACF report writer immediately and returns control to the control program (CP) on z/VM.

Phase 2

Record Selection:

During the second phase, *record selection*, the RACF report writer compares each record from the input file—the SMF records—against the criteria you specify on the SELECT and EVENT subcommands. The RACF report writer accepts as input only RACF-related SMF records. These are process records (SMF type 80 and 83) and status records (SMF type 81). In addition, the report writer generates a "fake" type 81 record for every SMF type 80 record that results from a SETROPTS or RVARY command.

For a description of SMF record types 80, 81, and 83, see *z/VM: RACF Security Server Macros and Interfaces*.

If you do not specify any SELECT or EVENT subcommands, the RACF report writer selects all of the records from the input file for further processing. If you specify options that limit your report, only limited information is saved.

Record Reformatting:

To sort and print the SMF input records, the RACF report writer must reformat them. The report writer allocates an in storage buffer for reformatting, using it on each SMF record being processed. The size of this buffer is determined by the WRKLRECL field in the installation-replaceable module ICHRSMFI unless LRECL is specified on SORTIN DD or SORTIN FILEDEF. The LRECL value in the SORTIN DD statement or the SORTIN FILEDEF overrides the WRKLRECL statement used by RACFRW.

In either case, the report writer makes sure that the buffer is large enough for the base section of the SMF record. However, it does not guarantee that the relocate sections of the SMF record will fit. For example, on z/VM if you need to increase the LRECL to 25000, you can change the FILEDEF for the SORTIN file in RACRPORT EXEC to:

```
FILEDEF SORTIN DISK SORT WORK A4 (RECFM V LRECL 25000 BLKSIZE 25000
```

In the report writer output, the process records that do not fit into the buffer will be noted as *truncated*. The status records that do not fit will be noted as *bypassed*. The WRKLRECL default is 4096.

The RACF report writer copies the records to a CMS file. (During its execution, the RACRPORT EXEC asks you whether you want to place this CMS file on the T-disk or the A-disk.) This file is saved until it is overwritten by a subsequent invocation of the report writer, or until it is erased.

If the input consists of records previously saved using the report writer, those records are already reformatted. The RACF report writer skips the reformatting step for those records. Operands on the RACFRW command specify whether or not the RACF report writer is to reformat the input records and whether or not the work data set is to be saved for subsequent runs of the RACF report writer.

When the RACF report writer has compared all of the input records against the selection criteria and, if necessary, reformatted the selected records and copied them to a work data set or CMS file, the second processing phase is complete.

Phase 3

Report Generation:

During the third phase, *report generation*, the RACF report writer generates the reports that you request with the LIST and SUMMARY subcommands. It uses as input only the records from the CMS file on z/VM. The RACF report writer always produces a header page with a list of the subcommands that you have entered and describes the meanings of values for such activities as job initiation, logon, resource access, and use of RACF commands that appear in the reports. The other reports depend on operands you have specified, but the RACF report writer always produces the reports you request according to a specific order. See the examples at the end of this chapter.

If you want a general summary report of overall system activity related to RACF, you can specify the GENSUM operand on the RACFRW command. The RACF report writer collects the data for the general summary report during phase 2 (the record selection phase) and prints it before any other reports during phase 3.

Next, the RACF report writer produces reports for the LIST subcommand and lists all SMF records from the work data set in the sequence that you have specified. Finally, for each SUMMARY subcommand you enter with a RACFRW command, the report writer produces a separate summary report of the SMF records by group, resource, command, RACF event, or owner activity (depending on what you specified for SUMMARY).

Sample reports produced by GENSUM, LIST, and SUMMARY appear at the end of this chapter. When it has completed the last report, the RACF report writer terminates and returns control to the invoker of the RACRPORT EXEC.

RACF Report Writer Command and Subcommands

The following tables summarize the main RACFRW command operands and subcommands that control report writer processing:

Table 7. Summary of RACFRW Command and Its Operands

Operand	**Result**
GENSUM	Produces a general summary report of system activity related to RACF
NOGENSUM	Produces no general summary report
FORMAT	Specifies that SMF records are to be formatted for use by the report writer
NOFORMAT	Specifies that the input SMF records are already formatted for use by the report writer; no reformatting is necessary
SAVE	On z/OS, saves the reformatted records on a work data set. Only those records that satisfy the specified SELECT/EVENT criteria are saved. Does not apply to z/VM because z/VM input records are automatically saved in a work file defined during RACF installation.

Table 8. Summary of RACFRW Subcommands

Subcommand	**Result**
SELECT	Specifies which SMF records to choose from the input file for report writer processing
EVENT	Specifies further which SMF records to choose from the input file; for the report writer to process these records, each record must meet the criteria
LIST	Specifies that the report writer is to list each record that is processed by SELECT/EVENT groups
SUMMARY	Specifies that the report writer is to print summary reports for records processed by SELECT/EVENT groups

Table 8. Summary of RACFRW Subcommands (continued)	
Subcommand	**Result**
END	Terminates subcommand processing

Planning Considerations

To use the RACF report writer at your installation, you must have:

- An output device that can handle 133 character lines.

RACF Report Writer Return Codes

Upon completion, the RACF report writer returns control to the user who entered RACRPORT on z/VM, with a return code in register 15.

The following are possible return codes:

Return Code
Meaning

0
The report writer has terminated normally.

12
The report writer has not terminated successfully for one of the following reasons:

- It could not dynamically allocate any needed resource that was not preallocated by the user
- It could not open any needed resource
- It received a nonzero return code from a service routine that it has invoked
- It received a nonzero return code from the SORT/MERGE routines.

If you receive a return code of 12, check to see whether any error messages were issued when you invoked the report writer.

The contents of register 15 are placed in the CMS ready message (Rxxxxx), where xxxxx is a nonzero return code. If you receive a return code of 12 while running the report writer on z/VM, check to see that the batch console was spooled back to your reader and that you have entered SET EMSG ON before you invoke the RACRPORT EXEC.

For more information on report writer error messages, see *z/VM: RACF Security Server Messages and Codes*.

Useful Hints

When you use the RACF report writer, consider the following:

- In an installation using RACF to protect multiple systems, each system writes RACF-generated SMF records to a different file. You can concatenate all of these files into a single file for input to the RACF report writer. Later, should you have to separate the information based on the identifier of the system that generated it, you could use the SYSID operand on either the LIST or the SELECT subcommand.
- If your installation is using multiple RACF service machines and you have a RACFSMF user ID defined, individual SMF files are stored on the SMF archive disk, RACFSMF's 192 by default, for each service machine. Make sure that you process all of these files for audit purposes.
- Your system programmer can provide special SMF record selection and tailoring by using the RACF report writer exit routine ICHRSMFE. For more information, see *z/VM: RACF Security Server System Programmer's Guide*.
- The RACF report writer runs as a postprocessor of RACF and does not interfere with normal RACF processing.

RACFRW Command

This section shows the function and syntax of the RACF report writer command (RACFRW) and subcommands (SELECT, EVENT, LIST, SUMMARY, and END). The command and subcommands are not listed alphabetically, but in the order in which you are likely to enter them. This order is: RACFRW, SELECT, EVENT, LIST, SUMMARY, and END.

The following key defines the symbols used in this chapter to represent the syntax of the command and subcommands:

UPPERCASE
characters must appear as shown

lowercase
characters indicate that the user supplies the information

list...
indicates that the item can be listed more than once

{ }
group alternative items; you can only specify one item

[ ]
indicates an optional item that you can specify

KEYWORD
indicates the default when no item is specified

Figure 26. Key to Symbols in Command Definitions

To initiate the report writer you must invoke the RACRPORT EXEC. The RACFRW CONTROL file must contain the input required by the report writer, including the RACFRW command and subcommands.

On the RACFRW command, you can specify the source and disposition of input records, the data to be passed to the installation-wide exit routine (ICHRSMFE), whether or not the RACF report writer is to reformat the input records, and whether or not the RACF report writer is to print a general summary report. (See *z/VM: RACF Security Server System Programmer's Guide* for further information about the installation-wide exit ICHRSMFE.)

The syntax of the RACFRW command is

```
RACFRW        [TITLE('q-string')]

              [DATA('q-string')]

              [{FORMAT  }]
              [{NOFORMAT}]

              [LINECNT( {  60  } ) ]
              [         {number}   ]

              [{GENSUM  }]
              [{NOGENSUM}]
```

TITLE('q-string')
specifies a string of up to 132 characters, enclosed in single quotation marks, to be used as a default heading for the report pages, if the TITLE operand on either the SUMMARY or LIST subcommand does not specify a unique report heading for a requested report.

DATA('q-string')
specifies a string of up to 256 characters of data, enclosed in single quotation marks, to be passed to the installation-wide exit routine (ICHRSMFE).

FORMAT
specifies that the RACF SMF records used as input to the RACF report writer must be reformatted (from the way they appear in the SMF records) before processing. For additional information about the reformatted records, see *z/VM: RACF Security Server System Programmer's Guide*. FORMAT implies

that the RACF report writer has not previously processed the input records. FORMAT is the default value.

NOFORMAT
specifies that the RACF SMF records used as input to the RACF report writer are already reformatted and suitable for processing. NOFORMAT implies that the input records have been processed previously by the RACF report writer and saved. Input records are saved automatically in a work file defined during RACF installation.

Note: Specifying FORMAT for a data set that is already reformatted or specifying NOFORMAT for a data set that is not already reformatted can cause unpredictable results.

If report writer input is from SMF, records are not reformatted. If input is a file saved from a previous report writer run, records are reformatted.

Restriction: If records have been reformatted and saved using the SAVE operand on one release of RACF report writer, the same release must be used to process the saved reformatted records. For example, RACF 1.8 reformatted records must be processed with RACF 1.8. SMF records from previous RACF releases, however, are supported. If you want to process SMF data from previous releases, archive the original SMF records rather than the reformatted records.

LINECNT(number)
specifies the maximum number of lines to be written before ejecting to a new page. The minimum number that you can specify is 20. If you specify a number lower than 20, LINECNT defaults to 20. If you omit this operand, LINECNT defaults to 60.

GENSUM
specifies that a general summary report is to be printed. This report contains various statistics about all the RACF SMF records processed, such as total JOB/LOGON attempts, successes, and violations, total resource accesses, successes, and violations, and a breakdown of JOB/LOGON and resource access violations by hour.

NOGENSUM
specifies that a general summary report is not to be printed. NOGENSUM is the default value.

RACFRW Subcommands

On z/VM, the subcommands must be in the CMS file RACFRW CONTROL.

SELECT Subcommand

The SELECT subcommand allows you to choose specific records from the input file containing the RACF SMF records. The RACF report writer reformats these selected records, if necessary, and copies them to a CMS file. Although all input records are used for the general summary report, the RACF report writer can list and generate summary reports for only the records that are indicated on the SELECT subcommand.

Note: RACF reports are only as good as the SMF records used as input to them. You need to carefully consider your installation's needs when selecting audit options and be sure the report writer has enough data to make useful reports.

SELECT/EVENT Groups

SELECT and EVENT subcommands provide a way to tailor RACF report writer output. It is easier for you to review a few, selected reports than to examine all the data at once. SELECT and EVENT commands work together to restrict the SMF records that the report writer uses for input. You can run the report writer several times on the same SMF data using different SELECT and EVENT criteria to obtain several reports on specific topics. You can issue SELECT subcommand separately or with EVENT subcommands to form what is called a SELECT/EVENT group.

For each run of the report writer, you can specify zero or more SELECT/EVENT groups. Each group consists of a SELECT subcommand followed by zero or more EVENT subcommands. A second SELECT subcommand indicates the beginning of another group.

For an SMF record to be used in a RACF report, it must meet the criteria of at least one of the SELECT/EVENT groups. The SMF record must meet all the criteria of the SELECT subcommand plus all the criteria of at least one of the EVENT subcommands in that group.

A SELECT/EVENT group must begin with a SELECT subcommand, even if it is a SELECT subcommand with no operands. You can then follow this subcommand with up to 49 EVENT subcommands that specify additional selection criteria for that group. If you do not specify an EVENT subcommand, RACF uses only the criteria from the SELECT subcommand. See "EVENT Subcommand" later in this chapter.

If you specify multiple SELECT subcommands or SELECT/EVENT groups or both, you can specify the groups in any order. The listing and summary reports that you request, however, will reflect *all* the records that have been selected by *all* the groups, not just the records selected by one particular SELECT/EVENT group. If you do not issue any SELECT subcommands or SELECT/EVENT groups, *all* the RACF SMF records from the input file are selected.

The RACF report writer can process a maximum of 50 SELECT and EVENT subcommands.

The following example produces a listing of all unsuccessful logons and all successful SETROPTS commands.

```
RACFRW
SELECT VIOLATIONS
EVENT LOGON
SELECT SUCCESSES
EVENT SETROPTS
LIST
END
```

The next example provides a listing of every unsuccessful RACF event (logons, accesses, SVCs, commands) plus successful logons and successful SETROPTS commands.

```
RACFRW
SELECT VIOLATIONS
SELECT SUCCESSES
EVENT LOGON
EVENT SETROPTS
LIST
END
```

The following example results in a listing of every RACF-related SMF record.

```
RACFRW
LIST
END
```

Note: Use a comma to separate items in a list of operands for SELECT or EVENT. If you must continue items in a list on another line, no continuation character is necessary.

```
SELECT  DATE(89195:89197)  TIME(010000:120000) USER(user1,user2,
user3,user4,user5)
```

See the syntax of the SELECT and EVENT subcommands for those operands that allow you to specify lists of items.

The syntax of the SELECT subcommand is

```
{SELECT}   [DATE  {(begin-number:end-number)} ]
{SEL   }   [      {(number-list...)         } ]

           [TIME  {(begin-number:end-number)} ]
           [      {(number-list...)         } ]

           [{VIOLATIONS}]
           [{SUCCESSES }]
           [{WARNINGS  }]

           [{USER(name-list...)}]
           [{NOUSER            }]

           [{OWNER(name-list...)}]
           [{NOOWNER            }]

           [GROUP(name-list...)]

           [{STATUS}]
           [{PROCESS}]

           [SYSID(value-list...)]

           [ AUTHORITY( [NORMAL] [SPECIAL]     ]
           [            [OPERATIONS] [AUDITOR] ]
           [            [EXIT] [FAILSOFT]      ]
           [            [BYPASSED] )                    ]

           [ REASON( [CLASS] [USER] [SPECIAL]      ]
           [         [RESOURCE] [RACINIT]          ]
           [         [COMMAND] [CMDVIOL] [AUDITOR] ]
           [         [SECAUDIT] [VMAUDIT]          ]
           [         [SECLABELAUDIT] [LOGOPTIONS]  ]
           [         [COMPATMODE] )                          ]

           [TERMINAL(name-list...)]
```

DATE(begin-number:end-number) or DATE(number-list...)
specifies a range (in ascending order) or a list of dates in the form YYDDD that are to be selected for further processing.

TIME(begin-number:end-number) or TIME(number-list...)
specifies a range (in ascending order) or a list of times in the form HHMMSS that are to be selected for further processing.

VIOLATIONS
specifies that only records identifying security violations are to be selected for further processing. This field applies to PROCESS records only.

SUCCESSES
specifies that only records identifying successful access attempts are to be selected for further processing. SUCCESSES applies to PROCESS records only.

WARNINGS
specifies that only records for which a warning message was issued are to be selected for further processing. This field applies to PROCESS records only.

If you do not specify VIOLATIONS, SUCCESSES, or WARNINGS, none of these is used as a selection criterion.

USER(name-list...)
specifies a list of user IDs that are to be selected for further processing. USER applies to PROCESS records only. If you omit both the USER and NOUSER operands, the RACF report writer selects all records containing user IDs. (See Notes 1 and 2.)

NOUSER
specifies that records that contain user IDs are not to be selected for further processing. If you omit both the USER and NOUSER operands, the RACF report writer selects all records containing user IDs.

If you specify both the NOUSER and NOJOB operands, the RACF report writer ignores both operands. (See Notes 1 and 2.)

OWNER(name-list...)
specifies a list of resource owner names that are to be selected for further processing. OWNER applies to PROCESS records only. If you omit both the OWNER and NOOWNER operands, owner is not a selection criterion.

NOOWNER
specifies that records that contain resource owner names are not to be selected for further processing. If you omit both the OWNER and NOOWNER operands, owner is not a selection criterion.

GROUP(name-list...)
specifies a list of group names that are to be selected for further processing. GROUP applies to PROCESS records only. (See Note 1.)

STATUS
specifies that only STATUS records are to be selected for further processing. STATUS records are RACF SMF record types 80 (generated by the SETROPTS or RVARY command) and 81.

PROCESS
specifies that only SMF record types 80 and 83 are to be selected for further processing.

SYSID(value-list...)
specifies a list of system identifiers that are to be selected for further processing.

AUTHORITY(type...)
specifies a list of authority types that are to be selected for further processing. AUTHORITY applies to PROCESS records only. Type can be any of the following:

SPECIAL
Selects records produced because the user had the SPECIAL or group-SPECIAL attribute

OPERATIONS
Selects records produced when access was granted because the user had the OPERATIONS or group-OPERATIONS attribute

AUDITOR
Selects records produced because the user had the AUDITOR or group-AUDITOR attribute

EXIT
Selects records produced when access was granted by an installation-wide exit routine

NORMAL
Selects records produced when access was granted for a reason other than those listed above (for example, when the user had sufficient access authority)

FAILSOFT
Selects records produced when failsoft processing was in effect

BYPASSED
Selects records produced because of accesses in which RACF authority checking was bypassed because BYPASS was specified on the user ID

REASON(value...)
specifies the reasons for logging the records that are to be selected for further processing. The REASON operand applies to PROCESS records only. Its value can be any of the following:

CLASS
Selects records produced because auditing of profile changes was in effect for a particular class. This record was produced because SETROPTS AUDIT was in effect.

USER
Selects records produced because auditing was in effect for the specific users. This record was produced because UAUDIT was specified for the user.

SPECIAL
Selects records produced because auditing was in effect for SPECIAL or group-SPECIAL users. This record was produced because SETROPTS SAUDIT was in effect.

RESOURCE
Selects records produced because auditing was in effect for the specific resource or because a RACHECK installation-wide exit routine requested auditing. (See Note 3.)

RACINIT
Selects records produced by a RACINIT request.

COMMAND
Selects records produced by commands that are always logged.

CMDVIOL
Selects records produced because auditing of command violations was in effect. This record was produced because SETROPTS CMDVIOL was in effect.

AUDITOR
Selects records produced because auditing of the specific resource was in effect. This record was produced because GLOBALAUDIT was specified in the profile. (See Note 3.)

SECAUDIT
Selects records produced because auditing of resources according to SECLEVEL was in effect. This record was produced because SETROPTS SECLEVELAUDIT was in effect.

VMAUDIT
Selects records produced because auditing of specific z/VM events was in effect.

SECLABELAUDIT
Selects records produced because auditing of resources according to SECLABEL was in effect.

LOGOPTIONS
Selects records produced because LOGOPTIONS auditing was in effect for a particular class.

COMPATMODE
Selects records produced because SETROPTS COMPATMODE was in effect.

TERMINAL(name-list...)
specifies a list of terminal IDs that are to be selected for further processing. TERMINAL applies to PROCESS records only.

Note:

1. If the user name is available in the relocate section of SMF record type 80, RACF includes it in both the PROCESS records listing and the SUMMARY reports.
2. The RACF report writer can select a record because of either RESOURCE or AUDITOR or both RESOURCE and AUDITOR.

EVENT Subcommand

The EVENT subcommand allows you to specify selection criteria related to particular RACF events. For a record to be selected for further processing by the RACF report writer, it must satisfy *all* the selection criteria that you specify on this EVENT subcommand.

You can use the EVENT subcommand only with a SELECT subcommand in a SELECT/EVENT group. With the EVENT subcommand, you can create a subset of the records that have already met the selection criteria specified on the SELECT subcommand. (“SELECT Subcommand” on page 97 describes SELECT/EVENT groups in more detail.)

The EVENT subcommand applies to PROCESS records only.

The syntax of the EVENT subcommand is

```
{EVENT}          event-name
{EV   }

                 [EVQUAL(value-list...)]

                 [CLASS(name-list...)]

                 [NAME(name-list...)]

                 [DSQUAL(name-list...)]

                 [INTENT( [ALTER] [CONTROL] [UPDATE] ]
                 [        [READ]   [NONE] )          ]

                 [ALLOWED( [ALTER] [CONTROL] [UPDATE] ]
                 [          [READ]  [NONE] )          ]

                 [NEWNAME(name-list...)]

                 [NEWDSQUAL(name-list...)]

                 [        {begin-number:end-number}   ]
                 [ LEVEL( {                       } ) ]
                 [        {number-list...         }   ]
```

event-name
specifies one of the following valid event names: An asterisk (*) after the event name indicates that the name is used on z/OS systems only because the functions are not performed on z/VM.

LOGON
z/VM logon

ACCESS
Access to a RACF-protected resource

Note: You can obtain SETEVENT records by specifying the VMXEVENT resource class.

ADDVOL *
Add a volume to a multivolume data set or tape volume set

RENAME
Rename a data set, SFS file, or SFS directory

DELETE
Delete a resource

DELVOL *
Delete one volume of a multivolume data set or tape volume set

DEFINE
Define a resource

ALLSVC
All of the preceding functions (ACCESS, ADDVOL, RENAME, DELETE, DELVOL, and DEFINE)

ADDSD
ADDSD command

ADDGROUP
ADDGROUP command

ADDUSER
ADDUSER command

ALTDSD
ALTDSD command

ALTGROUP
ALTGROUP command

ALTUSER
ALTUSER command

CONNECT
CONNECT command

DELDSD
DELDSD command

DELGROUP
DELGROUP command

DELUSER
DELUSER command

PASSWORD
PASSWORD command

PERMIT
PERMIT command (including PERMDIR and PERMFILE)

RALTER
RALTER command (including ALTDIR and ALTFILE)

RDEFINE
RDEFINE command (including ADDDIR and ADDFILE)

RDELETE
RDELETE command (including DELDIR and DELFILE)

REMOVE
REMOVE command

RVARY
RVARY command

SETROPTS
SETROPTS command

ALLCOMMAND
All of the preceding RACF commands (ADDSD through SETROPTS)

APPCLU
Partner LU verification through use of APPCLU profile.

GENERAL
General purpose auditing

Not all of the EVENT subcommand operands are valid with certain event names. Use Table 9 on page 103 to determine which event name and operand combinations are valid.

Table 9. EVENT Subcommand Operand Combination Table

Event Name	Event Code	EVQUAL	CLASS	NAME	DSQUAL	INTENT	ALLOWED	NEWNAME	NEWDSQUAL	LEVEL
LOGON	1	X								
ACCESS	2	X	X	X	X	X	X			X

Table 9. EVENT Subcommand Operand Combination Table (continued)

Event Name	Event Code	EVQUAL	CLASS	NAME	DSQUAL	INTENT	ALLOWED	NEWNAME	NEWDSQUAL	LEVEL
ADDVOL	3	X	X	X	X		X			X
RENAME	4	X		X	X			X	X	X
DELETE	5	X	X	X	X					X
DELVOL	6	X	X	X	X					X
DEFINE	7	X	X	X	X					X
ALLSVC	2-7	X	X	X	X	X	X	X	X	X
RACF Commands	8-25	X	X[1]	X	X[2]					
ALL COMMAND	8-25	X	X	X	X					
APPCLU	26	X	X	X						X
GENERAL	27	X	X							

Note:

1. CLASS is valid for the PERMIT, RALTER, REDEFINE, and RDELETE commands only.
2. DSQUAL is not valid for the RDEFINE, RALTER, and RDELETE commands.

EVQUAL(value-list...)
specifies a list of event qualifiers to be selected. Table 9 on page 103 lists the valid event qualifiers for each event name. Figure 28 on page 118, which shows the contents of the header page, identifies the meaning of each event qualifier.

CLASS(class-name...)
specifies a list of resource class names to be selected. Only the DATASET class and class names found in the class descriptor table are valid.

Note: RACF includes use of the SETEVENT command under the VMXEVENT resource class. See Table 9 on page 103 for the event names that are valid with the CLASS operand.

NAME(name-list...)
specifies a list of resource names to be selected. In the NAME field, you must specify a fully-qualified data set name, *not* a profile name for RACF SVC events (ACCESS, ADDVOL, RENAME, DELETE, DELVOL, DEFINE, ALLSVC). On the other hand, you must specify a profile name, *not* a fully-qualified data set

name, in the NAME field for RACF command events (ADDSD, ALTDSD, DELDSD, PERMIT, RALTER, RDEFINE, RDELETE, ALLCOMMAND).

To select specific data sets, you must specify fully-qualified dataset names in the 'name-list'. Also, if a dataset has been renamed and you want to use this operand to select the old dataset name, you must specify the fully-qualified, old data set name in the 'name-list'. This operand is not valid with the LOGON event name. You can specify generic names if you are looking for commands issued against that profile.

INTENT
specifies a list of intended access authorities to be selected. An intended access authority is the minimum authority needed by a user to access a particular resource (not the actual authority held by the user). The valid intended access authorities are ALTER, CONTROL, UPDATE, READ, and NONE. The INTENT operand is valid only with the ACCESS event name.

ALLOWED
specifies a list of allowed access authorities to be selected. An allowed access authority is the actual authority held by the user requesting access to a particular resource (not the minimum authority needed by the user to access that resource). The valid, allowed access authorities are ALTER, CONTROL, UPDATE, READ, and NONE. The ALLOWED operand is valid only with either the ACCESS or the ADDVOL event names.

NEWNAME(name-list...)
specifies a list of new, fully-qualified resource names to be selected. This operand is valid only with the RENAME event name.

LEVEL(begin-number:end-number) or LEVEL(number-list)
specifies a range (in ascending order) or a list of resource levels to be selected.

The meaning of the level indicator is set by your installation with the ADDSD, ALTDSD, RDEFINE, and RALTER commands. See the *z/VM: RACF Security Server Command Language Reference* for more information about the LEVEL operand. Table 9 on page 103 shows the event names that are valid with the LEVEL operand.

LIST Subcommand

The LIST subcommand formats and prints a listing of each individual RACF SMF record (both PROCESS and STATUS) that passes the selection criteria specified on the SELECT and EVENT subcommands. On the LIST subcommand, you can specify the title, sort sequence, and format control for the listing. The RACF report writer processes only one LIST subcommand at a time; if you enter more than one, the RACF report writer recognizes only the last LIST subcommand that you have entered. (The RACF report writer does all processing after you enter the END command.)

If you want to execute a LIST subcommand more than once to produce your reports, you must run the report writer each time. If you use the same selection criteria for each LIST subcommand you run, use the SAVE operand on RACFRW to specify the work-data set that is to contain the selected, reformatted SMF records. In this way, you can avoid unnecessary processing each time you run the report writer.

The syntax of the LIST subcommand is

```
{LIST}       [TITLE('q-string')]
{L   }

             [SORT( [DATE] [TIME] [SYSID]      ]
             [      [USER] [GROUP] [EVENT]     ]
             [      [EVQUAL] [TYPE] [NAME]     ]
             [      [CLASS] [TERMINAL] [JOBID] ]
             [      [OWNER] [SECLABEL] )       ]

             [{ASCEND }]
             [{DESCEND}]

             [NEWPAGE]
```

TITLE('q-string')
specifies a string of up to 132 characters, enclosed in single quotation marks, to be used as the heading for each page of this particular listing. If you omit this operand but specify a default heading in the TITLE operand of the RACFRW command, the default heading appears on each page of the listing. If you omit both this operand and the RACFRW TITLE operand, no heading at all appears on the listing.

SORT(field-list)
specifies the fields of the input record (a reformatted RACF SMF record) that are to be used for sorting. If you specify the LIST subcommand without specifying the SORT operand, the RACF report writer sorts the records by RCDTYPE, at offset 5(5) in the reformatted SMF record, with STATUS records preceding PROCESS records. If you specify SORT operand values, the records are then further sorted within the STATUS and PROCESS groups by the fields that you specify on the SORT operand.

The sequence in which you specify the SORT operands determines the sequence in which the RACF report writer sorts the records. For example, specifying SORT(OWNER GROUP USER DATE TIME) causes the RACF report writer to sort according to the profile owner first, then the group name, then the user name. If you omit the SORT operand, the order in which the records were written to SMF is not necessarily the order in which the records appear in the output listing, unless you have specified EQUALS in the SORTEQU field of the installation-replaceable module (ICHRSMFI).

The following table describes the operands you can use to select a sort sequence. Even though these operands apply only to process records, specifying them does not affect the order of status records.

OPERAND	DESCRIPTION
DATE	Julian date (YYDDDF) that the job entered the system
TIME	Time of day (HHMMSSTH)
SYSID	System identifier
USER	User (job) names
GROUP	Group (step) names
EVENT	Security-event codes
EVQUAL	Security-event code qualifiers
TYPE	Event types: 1 = JOB/LOGON events 2 = SVC events 3 = command events
NAME	Names of resources within event types: user ID for JOB/LOGON events RESOURCE NAME for SVC and command events
CLASS	Resource class names
TERMINAL	Terminal ID
JOBID	Job ID from SMF job management record
OWNER	Owner of the resource
SECLABEL	Security label

ASCEND
specifies that the fields identified by the DATE and TIME operands are to be sorted in ascending order. If you omit the DATE and TIME operands, this operand is ignored.

ASCEND is the default value.

DESCEND
specifies that the fields identified by the DATE and TIME operands are to be sorted in descending order. If you omit both the DATE and TIME operands, this operand is ignored.

NEWPAGE
specifies that the listing is to start printing on a new page whenever the value in the major (first) sort field changes. If you omit the SORT operand, this operand is ignored.

SUMMARY Subcommand

The SUMMARY subcommand causes the RACF report writer to format and print reports that summarize the information in the RACF SMF records that meet the selection criteria on the SELECT and EVENT subcommands.

Using the SUMMARY subcommand, you can request reports that summarize the following:

- Group activity
- User activity
- Resource activity
- Security-event activity
- RACF command activity
- Owner activity
- Group activity broken down by resource
- User activity broken down by resource
- Resource activity broken down by user
- Resource activity broken down by group
- Resource activity broken down by security event
- Security event activity broken down by resource
- RACF command activity broken down by user
- RACF command activity broken down by group
- RACF command activity broken down by resource
- Owner activity broken down by resource.

On a SUMMARY subcommand, you can specify only one of the activities mentioned in the preceding list. You can, however, enter as many as 16 different SUMMARY subcommands for each RACFRW command. You can thus request reports of all possible activities in one run of the RACF report writer. (Note that, if you accidentally enter more than one SUMMARY subcommand for the same type of activity, it does not cause an error; the RACF report writer recognizes only the last one.) The order in which you enter the SUMMARY subcommands is the order in which the summary reports are printed.

The syntax of the SUMMARY subcommand is

```
{SUMMARY}      name1   [BY(name2)]
{SUM    }
               [ {VIOLATIONS} ]
               [ {SUCCESSES } ]
               [ {WARNINGS  } ]

               [NEWPAGE]

               [TITLE('q-string')]
```

name1
specifies the major field on which information is to be grouped and summarized. The valid values for name1 are: GROUP, USER, RESOURCE, EVENT, COMMAND, and OWNER.

BY(name2)
specifies a minor field within the major field on which information is to be grouped and summarized also. The valid values for name2 are: GROUP, USER, RESOURCE, and EVENT.

Note: Only the following single name and name1 [BY(name2)] combinations are valid:

Valid single names	Valid name1 [BY(name2)] combinations
GROUP	GROUP BY(RESOURCE)
USER	USER BY(RESOURCE)
RESOURCE	RESOURCE BY(USER)
EVENT	RESOURCE BY(GROUP)
COMMAND	COMMAND BY(EVENT)
OWNER	EVENT BY(RESOURCE)
	COMMAND BY(USER)
	COMMAND BY(RESOURCE)
	COMMAND BY(GROUP)
	OWNER BY(RESOURCE)

VIOLATIONS
specifies that only information about access violations is to be included in the summary.

SUCCESSES
specifies that only information about successful access attempts is to be included in the summary. If you omit VIOLATIONS, SUCCESSES, and WARNING, the summary includes information for both access violations and successful access attempts.

WARNINGS
specifies that only accesses that were successful only because WARNING mode was in effect are to be included in the summary. The information appears under the WARNINGS heading.

If you do not specify VIOLATIONS, SUCCESSES, or WARNINGS, the report summarizes all access attempts.

NEWPAGE
specifies that the summary report is to start printing on a new page whenever the value in name1 changes. NEWPAGE is valid only when BY(name2) is specified.

TITLE('q-string')
specifies a string of up to 132 characters, enclosed in single quotation marks, to be used as the heading for each page of this particular summary report. If you omit this operand but specify a default heading in the TITLE operand of the RACFRW command, the default heading appears on each page of the summary report. If you omit both this operand and the RACFRW TITLE operand, no heading at all appears on the summary report.

END Subcommand

The END subcommand terminates subcommand mode. All report-generation processing is done after you enter the END subcommand.

The syntax of the END subcommand is

```
END
```

Using the RACF Report Writer

Because of variations from one installation to another, it is not possible to identify all of the ways an auditor might use the RACF report writer. The following list, however, identifies some possibilities:

- "Monitoring Password Violation Levels" on page 109
- "Monitoring Access Attempts in WARNING Mode" on page 110
- "Monitoring Access Violations" on page 111
- "Monitoring the Use of RACF Commands" on page 111
- "Monitoring Specific Users" on page 112
- "Monitoring SPECIAL Users" on page 112
- "Monitoring OPERATIONS Users" on page 112
- "Monitoring Failed Accesses to Resources Protected by a Security Level" on page 113
- "Monitoring Accesses to Resources Protected by a Security Label" on page 113.

The following detailed descriptions of these tasks include brief examples of the report writer command and subcommands needed for each. (In the examples, lower case entries can be modified to suit the needs of your installation.) For sample reports, see "Sample Reports" on page 116.

Monitoring Password Violation Levels

Monitoring password violation levels enables you to:

- Determine how effectively new RACF users are coping with the LOGON process
- Determine if the number of password violations stabilizes over time
- Determine where (at which terminals) these password violations are occurring.

Note: The commands shown in the examples must be in the RACFRW control file against which RACRPORT is run.

To obtain a report that describes password violations, you can use the following command and subcommands:

```
RACFRW GENSUM...
SELECT PROCESS
EVENT LOGON EVQUAL(1)
LIST ...
END
```

Results

These subcommands create a general summary report and a listing of the selected process records. (See Figure 31 on page 120 and Figure 33 on page 122 for samples of the general summary report and listings of selected process records.)

The total number of logon violations in the general summary report includes all types of violations (invalid password, invalid group, and invalid terminal). Because the EVENT subcommand causes the RACF report writer to select only those process records that describe an invalid password, you can use the number of process records selected to determine the percentage of password violations. If, for example, the number of process records selected is 13 and the total number of job or logon attempts is 393, you can compute the percentage of password violations by dividing 13 by 393. In this particular example, the value is 3.3%.

The violation percentage is a useful number to record and track over time. As users become more familiar with using their user ID and password, this percentage should tend to stabilize at a relatively low level.

You can look at the terminal name in the listing of process records to determine where persistent violations are originating. The records selected are record type 80 (process records) with an event code of 1 for logon. (See Figure 28 on page 118 for a list of RACF events and their qualifiers.)

Monitoring Access Attempts in WARNING Mode

Your installation may choose to use warning mode during the initial implementation of RACF. During this period, resource profiles contain a warning indicator (specified when the owner creates or later changes the profile). When the warning indicator is set, RACF allows all requesters to access the resource, and, if the requester would not otherwise be allowed access, RACF sends a message to the requester. Logging occurs at the owner-specified access type and level.

If the owner of a resource has specified in the profile one of the following:

- AUDIT(FAILURE(READ))
- AUDIT(ALL(READ)) (or the defaults for these are in effect)

or if you, as auditor, specify one of the following:

- GLOBALAUDIT (FAILURE(READ))
- GLOBALAUDIT (ALL(READ))

RACF logs each access to the resource, and you can use the RACF report writer to provide a list of the accesses RACF allowed only because the warning indicator was set.

Using the warning indicator can help your installation to migrate gradually to RACF. Checking the requesters and resources in the report writer listing can enable you to develop access lists without disrupting authorized work and without the immediate need to write and test a RACF exit routine.

As the auditor, however, you must be aware that if your installation sets the warning indicator in a resource profile any requester can access the resource. You should verify that the profile for a highly classified resource (such as payroll or business-planning data) does not contain the warning indicator.

To obtain a list of the profiles in a particular class that have the warning indicator set, you can issue the RACF SEARCH command with the WARNING operand:

```
SEARCH  CLASS(class-name)  WARNING
```

For example, to list the profiles in the TERMINAL class that contain the warning indicator, enter:

```
SEARCH  CLASS(TERMINAL)  WARNING
```

To obtain a report of accesses granted only because the warning indicator was set, you can use the following command and subcommands:

```
RACFRW ...
 SELECT PROCESS WARNINGS
 LIST ...
END
```

Results

These subcommands produce a listing of the selected process records. The records selected are those that contain an event code of 2 for resource access and a qualifier from the table below.

EVENT NUMBER
DESCRIPTION

3
Warning issued because of access.

8
Warning issued because of missing security label from user or profile.

9
Warning issued because of insufficient security label authority.

13
Warning issued because of insufficient CATEGORY/SECLEVEL.

The WARNING indicator is also set in records for the following events: LOGON, RENAME, DEFINE.

Monitoring Access Violations

When warning mode is in effect, and during normal operation of RACF, it is essential to your job as an auditor that you be able to monitor access violations. RACF detects and logs an access violation when it denies a user access to a resource because that user is not authorized to access the resource. An access violation is, therefore, a symptom that someone either does not understand his or her role as a RACF user or is trying to bypass RACF protection. You can use a report of access violations to identify such users as well as to help your installation identify when it may need to change access lists or universal access codes (UACCs).

You can request the report for data set violations as well as for violations in any of the classes identified in the class descriptor table.

To obtain an access violation report, you can use the following command and subcommands with the resource classes for which you want information:

```
RACFRW ...
 LIST ...
  SELECT PROCESS
   EVENT ACCESS EVQUAL(1) CLASS(a valid resource class,...,
         a valid resource class)
   EVENT LOGON  EVQUAL(4)
END
```

Results

These subcommands create a listing of all process records that meet the criteria set in the EVENT subcommands. The EVENT ACCESS subcommand selects all process records that contain access violations for the specified classes (an event code of 2 and an event qualifier of 1). The EVENT LOGON subcommand expands the scope of the report to include all user attempts to log on from a terminal the user is not authorized to use (an event code of 1 and an event qualifier of 4).

Monitoring While Deferring Access Decisions

When installing RACF on a z/VM system, an installation can choose to defer access decisions to z/VM. That is, RACF allows z/VM to make the final access decision for some or all resources. This means that z/VM may grant access to a resource to which RACF would deny access. Auditing, however, remains unaffected by the deferring of access decisions. If you are logging access violations, RACF continues to log what it determines to be a violation, even though z/VM may authorize the access.

Monitoring the Use of RACF Commands

In any installation, the security administrator is probably the most frequent user of RACF commands. Occasionally, users without any privileged attributes may enter ADDSD, PERMIT, or RDEFINE, or another, similar command against one of their resources; however, some users may try to use the whole range of RACF commands. Unless the user is authorized, RACF does not execute the command. Each unauthorized attempt to use a RACF command, however, represents a potential security violation, an event that you should know about. You monitor the use of commands with the command-summary report.

To obtain a command-summary report, you can use the following command and subcommand:

```
RACFRW ...
 SUMMARY COMMAND BY (USER)
END
```

A sample command-by-user summary report appears in Figure 46 on page 128.

If you detect certain users making persistent, unauthorized use of RACF commands, you can extract the details of the commands used and the resources involved. To obtain details of any command violations logged for specific users, use the following command and subcommands:

```
RACFRW ...
SELECT VIOLATIONS USER(userid(s) ...)
LIST ...
END
```

Where *userid*(s) is the ID of the user making unauthorized use of RACF commands. Note that RACF does not automatically log the events that these reports describe. To obtain meaningful data, you must direct RACF to log the activities of specific users or command violations or both. The reports are useful only after RACF has logged the events for the time interval that is meaningful to you. See "Monitoring Specific Users" on page 112, "Monitoring SPECIAL Users" on page 112, and "Monitoring OPERATIONS Users" on page 112 for related information.

Monitoring Specific Users

If you have directed RACF, either through the UAUDIT operand on the ALTUSER command or the corresponding ISPF panel, to log the RACF-related activities of one or more specific users, you can use the report writer to obtain a listing of the activities of these users.

To obtain a listing of all records RACF has logged because you requested auditing of one or more specific users, you can use the following command and subcommands:

```
RACFRW ...
  SELECT PROCESS REASON(USER) ...
  LIST ...
END
```

Monitoring SPECIAL Users

If you have directed RACF, either through the SAUDIT operand on the SETROPTS command or the corresponding ISPF panel, to log the RACF-related activities of SPECIAL or group-SPECIAL users, you can use the report writer to obtain a listing of the activities of these users.

To obtain a listing of all records RACF has logged because you requested auditing of SPECIAL or group-SPECIAL users, you can use the following command and subcommands:

```
RACFRW ...
   SELECT PROCESS REASON(SPECIAL)
   SELECT PROCESS AUTHORITY(SPECIAL)
  LIST ...
END
```

Note the difference between REASON and AUTHORITY:

REASON
Shows why the SMF record was logged. REASON(SPECIAL) causes the report writer to select records logged because the SETROPTS SAUDIT operand was in effect.

AUTHORITY
Shows why RACF accepted a command as valid. AUTHORITY(SPECIAL) causes the report writer to select records logged because the command required the SPECIAL or group-SPECIAL attribute and the user had the required attribute.

Monitoring OPERATIONS Users

The OPERATIONS and group-OPERATIONS attributes are very powerful. OPERATIONS allows a user access to almost all resources. Group-OPERATIONS allows a user access to almost all resources within the scope of the group and its subgroups. (The only resources not accessible to the OPERATIONS or

group-OPERATIONS user are those that have been explicitly barred by placing the OPERATIONS user in the access list of a resource with an access level of NONE at either the user ID level or the group level.) Therefore, you should carefully monitor the activities of these users to ensure that all accesses to installation resources are for valid reasons.

To obtain a report of the activities of OPERATIONS and group-OPERATIONS users, you can use the following command and subcommand:

```
RACFRW ...
  LIST ...
   SELECT PROCESS AUTHORITY(OPERATIONS)
END
```

Note: RACF logs the activities of users with the OPERATIONS and group-OPERATIONS attributes if the following are true:

- The SETROPTS OPERAUDIT is in effect
- The access to the resource was successful because the user had the OPERATIONS or group-OPERATIONS attribute.

Monitoring Failed Accesses to Resources Protected by a Security Level

If you have directed RACF, through the SECLEVELAUDIT operand on the SETROPTS command or on the corresponding ISPF panel, to log accesses to resources that are protected by a security level, you can use the report writer to obtain a listing of any access attempts that have failed because the user did not have the sufficient security classification to access the resource.

When security-level auditing is in effect, RACF logs all attempts to access any resource protected by a given security level (such as "confidential") or higher. Therefore, you can create a report to list access violations to those protected resources and determine which users are attempting to access sensitive information at your installation.

To obtain a report of unauthorized access attempts to resources with a security-level classification, you can use the following command and subcommands:

```
RACFRW
   SELECT PROCESS REASON(SECAUDIT)
    EVENT ACCESS EVQUAL(6) CLASS(a valid resource class,. . .,
         a valid resource class)
 LIST
END
```

Result

These subcommands create a listing of all process records that have been logged because security-level auditing was in effect (REASON(SECAUDIT)) and meet the criteria set in the EVENT ACCESS subcommand (event code 2). The EVENT subcommand selects all failed attempts (event qualifier 6) to access any resource within the resource class that has a security level equal to or higher than the level specified on the SECLEVELAUDIT operand of the SETROPTS command or on the corresponding ISPF panel.

Monitoring Accesses to Resources Protected by a Security Label

If you have directed RACF, through the SECLABELAUDIT operand on the SETROPTS command or on the corresponding ISPF panel, to log accesses to resources that are protected by a security label according to the audit options in the SECLABEL profile, you can use the report writer to obtain a listing of all attempts to access the resource.

When the SECLABELAUDIT option is in effect, RACF logs accesses to resources by SECLABEL. Therefore, you can create a report to list attempts to access those protected resources and determine which users are attempting to access sensitive information at your installation.

To obtain a report of attempts to access resources with a security label, you can use the following command and subcommands:

```
RACFRW
   SELECT PROCESS REASON(SECLABELAUDIT)
    EVENT ACCESS
 LIST
END
```

Result

These subcommands create a listing of all process records that have been logged because the security-label auditing option was in effect (REASON(SECLABELAUDIT)) and meet the criteria set in the EVENT subcommand ACCESS (event code 2).

RACF Report Writer Examples

This section gives some examples of how to use the RACF report writer command and subcommands to produce various reports.

The first five examples show how to obtain single reports; however, to create all the reports that you require at your installation, you may need to execute the RACF report writer more than once. [2]

An execution of the RACF report writer consists of the RACFRW command, report definition subcommands, and the END subcommand. Example 6 shows how the report writer executed a series of subcommands to produce multiple reports that you did not intend to produce; example 7 shows how you can correct the subcommands to produce the number of reports you want.

Example 1—Obtaining a Report for All RACF SMF Records

To obtain a report of all RACF SMF records, listed in the order read from the input file, and a general summary report, showing overall RACF-related system activity, enter:

```
RACFRW TITLE('BIG LISTING') GENSUM
LIST
END
```

Example 2—Obtaining a Report for Minidisk Violations on z/VM

On z/VM, to obtain a report of all violations against minidisks owned by USERB in January 1989, sorted in date and time sequence, enter:

```
RACFRW TITLE('USERB MINIDISKS LIST REPORT')
SELECT VIOLATIONS DATE(89001:89031) OWNER (USERB)
EVENT ALLSVC CLASS(VMMDISK)
EVENT ALLCOMMAND CLASS(VMMDISK)
LIST SORT(DATE TIME)
```

To obtain a summary of this activity, enter:

```
SUMMARY RESOURCE BY(USER) TITLE('USERB VMMDISKS SUMMARY REPORT')
```

Example 3—Obtaining Multiple Reports the Wrong Way

[2] In z/VM the RACRPORT CONTROL file can have input for multiple executions of the RACF report writer. After you invoke the RACRPORT EXEC, the report writer continues running until all the commands and subcommands in RACRPORT CONTROL are executed.

Situation

Assume you need to produce the following separate reports:

- A detailed listing of all access violations, sorted by user
- A resource-by-user summary report, with totals for access violations only
- A listing of all successful accesses, sorted by date and time
- A resource-by-user summary report, with totals for successful accesses only.

You must produce these four *separate* reports because each report is to be distributed to four different people, each of whom is entitled to see only the information on one report.

Assume that you enter:

```
(1)
    RACFRW
(2)
    SELECT VIOLATIONS
(3)
    LIST TITLE('ACCESS VIOLATIONS LIST REPORT') SORT(USER)
(4)
    SUMMARY RESOURCE BY(USER) TITLE ('ACCESS VIOLATIONS SUMMARY REPORT')
(5)
    SELECT SUCCESSES
(6)
    LIST TITLE('ACCESS SUCCESS LIST REPORT') SORT(DATE TIME)
(7)
    SUMMARY RESOURCE BY(USER) TITLE('ACCESS SUCCESS SUMMARY REPORT')
(8)
    END
```

Result

Instead of receiving the four desired reports, you receive *two* reports:

- A list report of all violations and successes, sorted by date and time
- A summary report of resources-by-user, with both violations and successful accesses.

How RACF executed

Here is what happened:

- **RACF record selection**

  You intended to first select, list, and summarize only violations from the SMF input file (statements 2, 3, and 4). Second, you wanted to select, list, and summarize only successful accesses (statements 5, 6, and 7), and finally, you wanted to produce two summary reports, one for access violations and one for access successes (statements 4 and 7).

  However, the RACF report writer does not execute in that sequence. RACF first selects records based on *all* the SELECT and EVENT subcommands entered between the RACFRW command and the END subcommand. Only after this selection process is complete are any of the requested reports produced. In this example, the RACF report writer checked each record from the input file to see whether it was either an access violation (statement 2) or a successful access (statement 5). Because all of the SMF records met at least one of these conditions, the RACF report writer selected all of the records for further processing.
- **RACF LIST function**

The RACF report writer next produced a single list report (statement 6). RACF ignored the first LIST subcommand (statement 3) because only one LIST subcommand, the last one entered (statement 6), is valid for each execution of the RACF report writer. The report that was produced listed by date and time all the records selected (both access violations and successful accesses) as specified in statement 6.

- **RACF SUMMARY report**

  Next, the RACF report writer produced a single summary report (statement 7). Because the SUMMARY subcommand in statement 4 is the same as that in statement 7, RACF ignored the first SUMMARY subcommand and produced one summary report. If you enter identical SUMMARY subcommands between RACFRW and END, RACF only uses the last subcommand and produces one summary report.

  Thus, the single summary report for this example produced totals for all the records selected (both access violations and successful accesses).

Example 7—Obtaining Multiple Reports the Right Way

To produce the four listings that you intended, enter two separate RACFRW commands:

(1)

```
RACFRW
SELECT VIOLATIONS
LIST TITLE('ACCESS VIOLATIONS LIST REPORT') SORT(USER)
SUMMARY RESOURCE BY(USER) TITLE ('ACCESS VIOLATIONS SUMMARY REPORT')
END
```

(2)

```
RACFRW
SELECT SUCCESSES
LIST TITLE('ACCESS SUCCESS LIST REPORT') SORT(DATE TIME)
SUMMARY RESOURCE BY(USER) TITLE ('ACCESS SUCCESS SUMMARY REPORT')
END
```

After the first SELECT/LIST/SUMMARY subcommands (for RACFRW in statement 1), be sure to enter END. Next, execute the RACFRW command again (statement 2) for the second SELECT/LIST/SUMMARY subcommands and enter END. RACF interprets each RACFRW command separately and produces the four desired reports.

Sample Reports

This section includes examples of the various reports that you can request the RACF report writer to generate. Review each sample report to determine its usefulness to your particular installation.

The following list summarizes the sample reports and the command or subcommand you issue to request the report:

Figure	Report	Command/Subcommand Issued
Figure 27 on page 118	Summary Activity Report	From SMF
Figure 28 on page 118	Standard Header Page	Each time you invoke the RACF report writer, it produces a standard header page that lists the subcommands that you entered and describes the meanings of the event and event qualifier values used in the reports.

Figure	Report	Command/Subcommand Issued
Figure 31 on page 120	General Summary	RACFRW GENSUM
Figure 32 on page 121	Listing of Status Records (types 80 and 81)	LIST (see Note)
Figure 33 on page 122	Listing of Process Records (types 20, 30, 80 and 83)	LIST (see Note)
Figure 34 on page 123	Short User Summary	SUMMARY USER
Figure 35 on page 123	Short Group Summary	SUMMARY GROUP
Figure 36 on page 123	Short Resource Summary	SUMMARY RESOURCE
Figure 37 on page 124	Short Command Summary	SUMMARY COMMAND
Figure 38 on page 124	Short Event Summary	SUMMARY EVENT
Figure 39 on page 125	Short Owner Summary	SUMMARY OWNER
Figure 40 on page 125	User by Resource Summary	SUMMARY USER BY(RESOURCE)
Figure 41 on page 125	Group by Resource Summary	SUMMARY GROUP BY(RESOURCE)
Figure 42 on page 126	Resource by User Summary	SUMMARY RESOURCE BY(USER)
Figure 43 on page 126	Resource by Group Summary	SUMMARY RESOURCE BY(GROUP)
Figure 44 on page 127	Resource by Event Summary	SUMMARY RESOURCE BY(EVENT)
Figure 45 on page 127	Event by Resource Summary	SUMMARY EVENT BY(RESOURCE)
Figure 46 on page 128	Command by User Summary	SUMMARY COMMAND BY(USER)
Figure 47 on page 128	Command by Group Summary	SUMMARY COMMAND BY(GROUP)
Figure 48 on page 129	Command by Resource Summary	SUMMARY COMMAND BY(RESOURCE)
Figure 49 on page 129	Owner by Resource Summary	SUMMARY OWNER BY(RESOURCE)
Figure 50 on page 130Figure 51 on page 130Figure 52 on page 130	Listing of Process Records Listing of Process Records Listing of Process Records	LIST (see “Sample Report Writer Output for Shared User IDs” on page 129 for an explanation of shared user ID reports)

Note: A single LIST subcommand produces both the listing of status records and the listing of process records.

An explanation of the standard header page of the report is given in “Event Code Qualifiers ” on page 60. It documents *why* the event code qualifiers were set.

```
                                    SUMMARY ACTIVITY REPORT
START DATE-TIME  07/29/06-13:18:18                              END DATE-TIME  08/06/06-10:15:36
RECORD       RECORDS         PERCENT      AVG. RECORD   MIN. RECORD   MAX. RECORD       RECORDS
  TYPE          READ        OF TOTAL           LENGTH        LENGTH        LENGTH       WRITTEN
     0             2           .55 %            35.00            35            35             0
     2             0                                                                        1
     3             0                                                                        1
     4            41         11.33 %           251.48           207           263             0
     5            24          6.63 %           143.70           137           144             0
    20            52         14.36 %            94.23            91            98            52
    30           133         36.74 %           577.61           244         2,174           133
    80           108         29.83 %           450.78            80         1,685           108
    81             2           .55 %           756.00           756           756             2
TOTAL            362           100 %           402.00            35         2,174           297
NUMBER OF RECORDS IN ERROR             0
```

Figure 27. Summary Activity Report from SMF

```
2007.053 13:51:40                                        RACF REPORT
COMMAND GROUP ENTERED -
   RACFRW GENSUM
   LIST
   END
EVENT/QUALIFIER KEY ------
   EVENT  QUALIFIER  MEANING
     1               JOB INITIATION / TSO LOGON/LOGOFF
              0       SUCCESSFUL INITIATION
              1       INVALID PASSWORD
              2       INVALID GROUP
              3       INVALID OIDCARD
              4       INVALID TERMINAL/CONSOLE
              5       INVALID APPLICATION
              6       REVOKED USERID ATTEMPTING ACCESS
              7       USERID AUTOMATICALLY REVOKED
              8       SUCCESSFUL TERMINATION
              9       UNDEFINED USERID
             10       INSUFFICIENT SECURITY LABEL AUTHORITY
             11       NOT AUTHORIZED TO SECURITY LABEL
             12       SUCCESSFUL RACINIT INITIATION
             13       SUCCESSFUL RACINIT DELETE
             14       SYSTEM NOW REQUIRES MORE AUTHORITY
             15       REMOTE JOB ENTRY - JOB NOT AUTHORIZED
             16       SURROGAT CLASS IS INACTIVE
             17       SUBMITTER IS NOT AUTHORIZED BY USER
             18       SUBMITTER IS NOT AUTHORIZED TO SECURITY LABEL
             19       USER IS NOT AUTHORIZED TO JOB
             20       WARNING - INSUFFICIENT SECURITY LABEL AUTHORITY
             21       WARNING - SECURITY LABEL MISSING FROM JOB, USER, OR PROFI
             22       WARNING - NOT AUTHORIZED TO SECURITY LABEL
             23       SECURITY LABELS NOT COMPATIBLE
             24       WARNING - SECURITY LABELS NOT COMPATIBLE
             25       CURRENT PASSWORD HAS EXPIRED
             26       INVALID NEW PASSWORD
             27       VERIFICATION FAILED BY INSTALLATION
             28       GROUP ACCESS HAS BEEN REVOKED
             29       OIDCARD IS REQUIRED
             30       NETWORK JOB ENTRY - JOB NOT AUTHORIZED
             31       WARNING - UNKNOWN USER FROM TRUSTED NODE PROPAGATED
```

Figure 28. Standard Header Page (Part 1 of 3)

```
2007.053 13:51:40                                          RACF REPORT
      2              RESOURCE ACCESS
               0       SUCCESSFUL ACCESS
               1       INSUFFICIENT AUTHORITY
               2       PROFILE NOT FOUND - RACFIND SPECIFIED ON MACRO
               3       ACCESS PERMITTED DUE TO WARNING
               4       FAILED DUE TO PROTECTALL
               5       WARNING ISSUED DUE TO PROTECTALL
               6       INSUFFICIENT CATEGORY/SECLEVEL
               7       INSUFFICIENT SECURITY LABEL AUTHORITY
               8       WARNING - SECURITY LABEL MISSING FROM JOB, USER, OR PROFILE
               9       WARNING - INSUFFICIENT SECURITY LABEL AUTHORITY
              10       WARNING - DATA SET NOT CATALOGUED
              11       DATA SET NOT CATALOGUED
              12       PROFILE NOT FOUND - REQUIRED FOR AUTHORITY CHECKING
              13       WARNING: INSUFFICIENT CATEGORY/SECLEVEL
      3              ADDVOL/CHGVOL
               0       SUCCESSFUL PROCESSING OF NEW VOLUME
               1       INSUFFICIENT AUTHORITY
               2       INSUFFICIENT SECURITY LABEL AUTHORITY
               3       LESS SPECIFIC PROFILE EXISTS WITH DIFFERENT SECLABEL
      4              RENAME RESOURCE
               0       SUCCESSFUL RENAME
               1       INVALID GROUP
               2       USER NOT IN GROUP
               3       INSUFFICIENT AUTHORITY
               4       RESOURCE NAME ALREADY DEFINED
               5       USER NOT DEFINED TO RACF
               6       RESOURCE NOT PROTECTED
               7       WARNING - RESOURCE NOT PROTECTED
               8       USER IN SECOND QUALIFIER IS NOT RACF DEFINED
               9       LESS SPECIFIC PROFILE EXISTS WITH DIFFERENT SECLABEL
              10       INSUFFICIENT SECURITY LABEL AUTHORITY
              11       RESOURCE NOT PROTECTED BY SECURITY LABEL
              12       NEW NAME NOT PROTECTED BY SECURITY LABEL
              13       NEW SECLABEL MUST DOMINATE OLD SECLABEL
              14       WARNING - INSUFFICIENT SECURITY LABEL AUTHORITY
              15       WARNING - RESOURCE NOT PROTECTED BY SECURITY LABEL
              16       WARNING - NEW NAME NOT PROTECTED BY SECURITY LABEL
              17       WARNING - NEW SECLABEL MUST DOMINATE OLD SECLABEL
      5              DELETE RESOURCE
               0       SUCCESSFUL SCRATCH
               1       RESOURCE NOT FOUND
               2       INVALID VOLUME
      6              DELETE ONE VOLUME OF A MULTIVOLUME RESOURCE
               0       SUCCESSFUL DELETION
      7              DEFINE RESOURCE
               0       SUCCESSFUL DEFINITION
               1       GROUP UNDEFINED
               2       USER NOT IN GROUP
               3       INSUFFICIENT AUTHORITY
               4       RESOURCE NAME ALREADY DEFINED
               5       USER NOT DEFINED TO RACF
               6       RESOURCE NOT PROTECTED
               7       WARNING - RESOURCE NOT PROTECTED
               8       WARNING - SECURITY LABEL MISSING FROM JOB, USER, OR PROFILE
               9       WARNING - INSUFFICIENT SECURITY LABEL AUTHORITY
              10       USER IN SECOND QUALIFIER IS NOT RACF DEFINED
              11       INSUFFICIENT SECURITY LABEL AUTHORITY
              12       LESS SPECIFIC PROFILE EXISTS WITH DIFFERENT SECLABEL
```

Figure 29. Standard Header Page (Part 2 of 3)

```
2007.053 13:51:40                                          RACF REPORT
      8             ADDSD COMMAND
      9             ADDGROUP COMMAND
     10             ADDUSER COMMAND
     11             ALTDSD COMMAND
     12             ALTGROUP COMMAND
     13             ALTUSER COMMAND
     14             CONNECT COMMAND
     15             DELDSD COMMAND
     16             DELGROUP COMMAND
     17             DELUSER COMMAND
     18             PASSWORD COMMAND
     19             PERMIT COMMAND
     20             RALTER COMMAND
     21             RDEFINE COMMAND
     22             RDELETE COMMAND
     23             REMOVE COMMAND
     24             SETROPTS COMMAND
     25             RVARY COMMAND
              0       NO VIOLATIONS DETECTED
              1       INSUFFICIENT AUTHORITY
              2       KEYWORD VIOLATIONS DETECTED
              3       SUCCESSFUL LISTING OF DATA SETS
              4       SYSTEM ERROR IN LISTING OF DATA SETS
     26             APPCLU
              0       PARTNER VERIFICATION WAS SUCCESSFUL
              1       SESSION ESTABLISHED WITHOUT VERIFICATION
              2       LOCAL LU KEY WILL EXPIRE IN <= 5 DAYS
              3       PARTNER LU ACCESS HAS BEEN REVOKED
              4       PARTNER LU KEY DOES NOT MATCH THIS LU KEY
              5       SESSION TERMINATED FOR SECURITY REASON
              6       REQUIRED SESSION KEY NOT DEFINED
              7       POSSIBLE SECURITY ATTACK BY PARTNER LU
              8       SESSION KEY NOT DEFINED FOR PARTNER LU
              9       SESSION KEY NOT DEFINED FOR THIS LU
             10       SNA SECURITY RELATED PROTOCOL ERROR
             11       PROFILE CHANGE DURING VERIFICATION
             12       EXPIRED SESSION KEY
     27             GENERAL
           0-99       GENERAL AUDIT RECORD WRITTEN
-REPORT KEY ------
   .AN '*' PREFIXED TO A USER OR GROUP NAME INDICATES THE NAME IS ACTUALLY A JOB OR STEP NAME, RESPECTIVELY
   .THE PHRASE 'UNDEFINED USER' REFERS TO THOSE TSO LOGONS WHICH SPECIFIED USERIDS THAT WERE NOT DEFINED TO RACF,
    AND TO BATCH JOBS WHICH DID NOT SPECIFY THE 'USER=' OPERAND ON THEIR JOB STATEMENTS
   .A '+' PREFIXED TO A RESOURCE NAME INDICATES THAT A GENERIC PROFILE WAS ACCESSED
   .A '(G)' APPENDED TO A RESOURCE NAME MEANS THAT THE RESOURCE NAME IS GENERIC
   .A '-' APPENDED TO A VMXEVENT DESCRIPTION MEANS THAT THE EVENT CONTINUES ON THE NEXT LINE
```

Figure 30. Standard Header Page (Part 3 of 3)

```
2007.053 13:51:40                                RACF REPORT - GENERAL SUMMARY
                                                                 READ    SELECTED    %-SELECTED
STATUS RECORDS                                                     49          49      100 %
PROCESS RECORDS                                                   126         126      100 %
TOTAL PROCESS RECORDS FOR DEFINED USERS                           125         125       99 % (OF ALL PROCESS RECORDS)
TOTAL PROCESS RECORDS FOR UNDEFINED USERS                           1           1        1 % (OF ALL PROCESS RECORDS)
                                                 --- JOB / LOGON  STATISTICS ---
TOTAL JOB/LOGON/LOGOFF                                             19
TOTAL JOB/LOGON SUCCESSES                                           4                    21 % OF TOTAL ATTEMPTS
TOTAL JOB/LOGON VIOLATIONS                                         10                    53 % OF TOTAL ATTEMPTS
TOTAL JOB/LOGON ATTEMPTS BY UNDEFINED USERS                         1                     5 % OF TOTAL ATTEMPTS
TOTAL JOB/LOGON SUCCESSES BY UNDEFINED USERS                        0                     0 % OF TOTAL ATTEMPTS
TOTAL JOB/LOGON VIOLATIONS BY UNDEFINED USERS                       1                     5 % OF TOTAL ATTEMPTS
TOTAL JOB/LOGON SUCCESSFUL TERMINATION                              5
JOB/LOGON VIOLATIONS BY HOUR -
          0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8
            0           0           0           0           0           0           0           0
          8-9        9-10       10-11       11-12       12-13       13-14       14-15       15-16
            0           0           0           0          10           0           0           0
        16-17       17-18       18-19       19-20       20-21       21-22       22-23       23-24
            0           0           0           0           0           0           0           0
                                             --- RESOURCE  STATISTICS ---
TOTAL RESOURCE ACCESSES (ALL EVENTS)                               45
TOTAL RESOURCE ACCESS SUCCESSES                                    44                    98 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESS WARNINGS                                      0                     0 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESS VIOLATIONS                                    1                     2 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESSES (ALL EVENTS) BY UNDEFINED USERS             0                     0 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESS SUCCESSES BY UNDEFINED USERS                  0                     0 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESS WARNINGS BY UNDEFINED USERS                   0                     0 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESS VIOLATIONS BY UNDEFINED USERS                 0                     0 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESSES USING GENERIC PROFILE                       5                    11 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESS SUCCESSES USING GENERIC PROFILE               5                    11 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESS WARNINGS USING GENERIC PROFILE                0                     0 % OF TOTAL ACCESSES
TOTAL RESOURCE ACCESS VIOLATIONS USING GENERIC PROFILE              0                     0 % OF TOTAL ACCESSES
RESOURCE ACCESS VIOLATIONS BY HOUR -
          0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8
            0           0           0           0           0           0           0           0
          8-9        9-10       10-11       11-12       12-13       13-14       14-15       15-16
            0           0           0           0           1           0           0           0
        16-17       17-18       18-19       19-20       20-21       21-22       22-23       23-24
            0           0           0           0           0           0           0           0
```

Figure 31. General Summary Report

```
2007.053 13:51:40              RACF REPORT - LISTING OF STATUS RECORDS

 DATE   TIME     SYSID MISC. OPTIONS      EXITS    CLASS    PROT STAT AUD GEN GCMD GLBL GLST RLST LOPT
2007.053 12:17:41 R190  ORIGIN:   SETROPTS          DATASET  YES  YES  NO  YES YES  YES            DFLT
                        TERMUACC: READ              USER               NO
                        CMNDVIOL: YES               GROUP              NO
                        LOGSPEC:  YES               RVARSMBR YES  NO   NO  YES YES  YES            DFLT
                        RACINIT:  STATS             RACFVARS YES  NO   NO  YES YES            YES  DFLT
                        ADSP:     ACTIVE            SECLABEL YES  NO   NO  YES YES  YES            DFLT
                        REALDSN:  NO                DASDVOL  NO   NO   NO  YES YES  YES            DFLT
                        JES:                        GDASDVOL NO   NO   NO                         DFLT
                          BATCHALLRACF              TAPEVOL  YES  NO   NO  YES YES  YES            DFLT
                          XBMALLRACF                TERMINAL YES  NO   NO  YES YES  YES            DFLT
                          EARLYVERIFY               GTERMINL YES  NO   NO                         DFLT
                                                    APPL     NO   NO   NO  YES YES  YES            DFLT
                        TAPEDSN:  NO                TIMS     NO   NO   NO  YES YES  YES            DFLT
                        PROT-ALL: NO                GIMS     NO   NO   NO                         DFLT
                        PROGCTL:  NO                AIMS     NO   NO   NO  YES YES  YES            DFLT
                        OPERAUDIT:NO                TCICSTRN NO   NO   NO YES YES  YES            DFLT
                        ERASE:    YES               GCICSTRN NO   NO   NO                         DFLT
                          NOSECLEVEL                PCICSPSB NO   NO   NO  YES YES  YES            DFLT
                          ALL                       QCICSPSB NO   NO   NO                         DFLT
                        SECLEVELAUDITING INACTIVE   GLOBAL   NO   NO   NO                         DFLT
                        EGN:      INACTIVE          GMBR     NO   NO   NO  YES YES  YES            DFLT
                        SESSIONINTERVAL    30       DSNR     NO   NO   NO  YES YES  YES            DFLT
                        JES B1 SECURITY:            FACILITY NO   NO   NO  YES YES  YES            DFLT
                             NJEUSERID:  UNKUSER    VMMDISK  NO   NO   NO  YES YES  YES            DFLT
                          UNDEFINEDUSER: ++++++++   VMRDR    NO   NO   NO  YES YES  YES            DFLT
                        DEFAULT LANGUAGE CODES:     SECDATA  NO   NO   NO                         DFLT
                                 PRIMARY CODE: ENU PROGRAM  NO   NO   NO                         DFLT
                                SECONDARY CODE: ENU APPCLU   NO   NO   NO  YES YES  YES            DFLT
                        APPLAUDIT:  YES
                                                    JESJOBS  YES  NO   NO  YES YES  YES            DFLT
                                                    JESINPUT YES  NO   NO  YES YES  YES            DFLT
                                                    CONSOLE  YES  NO   NO  YES YES  YES        YES  DFLT
                                                    TEMPDSN  YES  NO   NO  YES YES  YES            DFLT
                                                    DIRAUTH  YES  NO   NO  YES YES  YES            DFLT
                                                    SURROGAT YES  NO   NO  YES YES  YES            DFLT
                                                    NODMBR   YES  NO   NO  YES YES  YES            DFLT
                                                    NODES    YES  NO   NO  YES YES            YES  DFLT
                                          OTHER OPTIONS -
                                            'LIST OF GROUPS' ACCESS CHECKING IS ACTIVE
                                            SINGLE LEVEL NAMES NOT ALLOWED
                                            INTERVAL:  253 DAYS
                                            HISTORY:  NONE
                                            REVOKE:   NO
                                            WARNING:  NONE
                                            INACTIVE:   NO
                                            NO PASSWORD SYNTAX RULES
                                          SECURITY OPTIONS:
                                            SECLABELCONTROL: INACTIVE
                                            CATDSNS:         INACTIVE
                                            MLQUIET:         INACTIVE
                                            MLSTABLE:        INACTIVE
                                            MLS:             INACTIVE
                                            MLACTIVE:        INACTIVE
                                            GENERICOWNER:    INACTIVE
                                            SECLABELAUDIT:   INACTIVE
                                            COMPATMODE:      INACTIVE
```

Figure 32. Listing of Status Records

If the LRECL value specified is too small, the report output contains the report heading and the following text:

```
**** STATUS RECORD BYPASSED; LRECL TOO SMALL ****
```

The LRECL value is obtained from the SORTIN DD statement or the WRKLRECL field in the ICHRSMFI module. See “Record Reformatting:” on page 93 for more details.

```
2007.053 13:51:40                          RACF REPORT - LISTING OF PROCESS RECORDS
                                                        E
                                                        V  Q
                                                        E  U
                                *JOB/USER  *STEP/   --TERMINAL--  N  A
 DATE    TIME   SYSID   NAME     GROUP      ID    LVL  T  L
2007.053 12:15:03 R190   IBMUSER   SYS1    LEO2      0   1  0  JOBID=(IBMUSER 90.053 12:15:01),USERDATA=(),OWNER=
                                                                AUTH=(NONE),REASON=(NONE)
2007.053 12:15:08 R190   IBMUSER   SYS1    LEO2      0   2  0  JOBID=(IBMUSER 90.053 12:15:01),USERDATA=(),OWNER=IBMUSER
                       GEORGE JONES                             AUTH=(NORMAL),REASON=(ENTITY OR FAILSOFT PROCESSING)
                                                                LOGSTR='LOGSTR DATA'
                                                                USER SECLABEL=SYSHIGH,SESSION=TSO LOGON,TERMINAL=LEO2
                                                                DATASET=SYS1.BROADCAST,GENPROF=SYS1.BRODCAST,VOLUME=SPOOL1,LEVEL=00
                                                                INTENT=READ,ALLOWED=ALTER
2007.053 12:17:33 R190   IBMUSER  SYS1     LEO2      0  10  0  JOBID=(IBMUSER 90.053 12:15:01).USERDATA=(),OWNER=IBMUSER
                       GEORGE JONES                             AUTH=(SPECIAL),REASON=(SPECIAL/OPERATIONS)
                                                                USER SECLABEL=SYSHIGH,SESSION=TSO LOGON,TERMINAL=LEO2
                                                                  ADDUSER RACFU01 DFLTGRP(SYS1) PASSWORD(****) NAME('
                                                                  ####################') AUTHORITY(USE) NOGRPACC UACC(NONE) NOADSP
                                                                  OWNER(IBMUSER) NOSPECIAL NOOPERATIONS NOCLAUTH NOAUDITOR NOOIDCARD
2007.053 12:17:41 R190   IBMUSER  SYS1     LEO2      0  24  0  JOBID=(IBMUSER 90.053 12:15:01),USERDATA=(),OWNER=
                       GEORGE JONES                             AUTH=(SPECIAL),REASON=(COMMAND)
                                                                USER SECLABEL=SYSHIGH,SESSION=TSO LOGON,TERMINAL=LEO2
                                                                  SETROPTS STATISTICS(DATASET)
2007.053 12:17:43 R190   IBMUSER  SYS1     LEO2      0   8  0  JOBID=(IBMUSER 90.053 12:15:01),USERDATA=(),OWNER=IBMUSER
                       GEORGE JONES                             AUTH=(SPECIAL),REASON=(SPECIAL/OPERATIONS)
                                                                USER SECLABEL=SYSHIGH,SESSION=TSO LOGON,TERMINAL=LEO2
                                                                  ADDSD IBMUSER.RACHECK.DATA UACC(NONE) SET
                                                                  NEW SECLABEL=NO SECLABEL,OLD SECLABEL=SYSHIGH
2007.053 12:17:44 R190   IBMUSER  SYS1     LEO2      0  19  0  JOBID=(IBMUSER 90.053 12:15:01),USERDATA=(),OWNER=IBMUSER
                       GEORGE JONES                             AUTH=(SPECIAL),REASON=(SPECIAL/OPERATIONS)
                                                                USER SECLABEL=SYSHIGH,SESSION=TSO LOGON,TERMINAL=LEO2
                                                                  PERMIT IBMUSER.RACHECK.DATA CLASS(DATASET)
                                                                  ID(RACFU01) ACCESS(READ)
2007.053 12:17:49 R190   IBMUSER  SYS1     LEO2      0  21  0  JOBID=(IBMUSER 90.053 12:15:01,USERDATA=(),OWNER=
                       GEORGE JONES                             AUTH=(SPECIAL),REASON=(SPECIAL/OPERATIONS)
                                                                USER SECLABEL=SYSHIGH,SESSION=TSO LOGON,TERMINAL=LEO2
                                                                  RDEFINE DIRECTRY FP.IBMUSER.DIR LEVEL(00) NONOTIFY
2007.053 12:20:09 R190   IBMUSER  SYS1     LEO2      0  15  0  JOBID=(IBMUSER 90.053 12:15:01),USERDATA=(),OWNER=IBMUSER
                       GEORGE JONES                             AUTH=(SPECIAL),REASON=(SPECIAL/OPERATIONS)
                                                                USER SECLABEL=SYSHIGH,SESSION=TSO LOGON,TERMINAL=LEO2
                                                                  DELDSD IBMUSER.NOACC.DATA SET
                                                                  NEW SECLABEL=SYSHIGH,OLD SECLABEL=NO SECLABEL
2007.053 12:26:42 R190  *IBMUSER  *RACFPROF FFFFFFF  0   1 11  JOBID=(IBMUSER 90.053 12:15:01),USERDATA=(),OWNER=
                                                                AUTH=(NONE),REASON=(RACINIT FAILURE)
                                                                USER SECLABEL=UNDEF,SESSION=TSO LOGON,TOKEN USER ATTRIBUTES=(
                                                                UNDEFINED USER),TERMINAL=FFFFFFF,SUBMITTING GROUP=GROUPA
2007.053 12:29:32 R190   IBMUSER   SYS1              0  13  0  JOBID=(IBMUSER 90.053 12:15:01),USERDATA=(),OWNER=IBMUSER
                       GEORGE JONES                             AUTH=(SPECIAL),REASON=(SPECIAL/OPERATIONS)
                                                                USER SECLABEL=SYSHIGH,TOKEN STATUS=(CREATED BY PRE 1.9 RACF CALL
                                                                  ALTUSER TSOG6 NOSECLABEL
                                                                  NEW SECLABEL=NO SECLABEL,OLD SECLABEL=L2C1
2007.053 12:29:56 R190   TSOG5     SYS1              0   1  1  JOBID=(IBMUSER 90.053 12:15:01),USERDATA=(),OWNER=
                       X                                        AUTH=(NONE),REASON=(RACINIT FAILURE)
                                                                USER SECLABEL=UNDEF
2007.053 12:36:49 R190   TSOG5     SYS1              0   1  1  JOBID=(IBMUSER 90.053 12:15:01),USERDATA=(),OWNER=
                       X                                        AUTH=(NONE),REASON=(RACINIT FAILURE)
                                                                USER SECLABEL=L1C1
2007.053 12:41:10 R190   IBMUSER   SYS1     LEO2     0   1  8  JOBID=(IBMUSER 90.053 12:15:01),USERDATA=(),OWNER=
                                                                AUTH=(NONE),REASON=(NONE)
2007.053 01:12:01 R190   *LISTBC    *               0   2  0  JOBID=(IBMUSER 90.053 12:15:01),USERDATA=(),OWNER=
                                                                AUTH=(TRUSTED),REASON=(LOGOPTIONS)
                                                                USER SECLABEL=SYSHIGH,SESSION=SYSTEM ADDRESS SPACE,
                                                                TOKEN=(DEFAULT TOKEN),TOKEN USER ATTRIBUTES=
                                                                (TRUSTED COMPUTER BASE) DATASET=BRODCAST.IBMUSER,
                                                                VOLUME=TEMP01,LEVEL=00,INTENT=ALTER,ALLOWED=ALTER
2007.053 01:24:53 R190   IBMUSER   SYS1              0   2  0  JOBID=(IBMUSERX 90.053 12:15:01),USERDATA=(),OWNER=IBMUSER
                                                                AUTH=(NORMAL),REASON=(LOGOPTIONS)
                                                                SESSION=INTERNAL READER BATCH JOB,JESINPUT=INTRDR,EXENODE=N1
                                                                SUBMITTING USER=IBMUSER,SUBMITTING NODE=N1,SUBMITTING
                                                                GROUP=SYS1 DATASET=SYS1.MANA,GENPROF=SYS1.*,VOLUME=PAGE08,
                                                                LEVEL=00,INTENT=READ,ALLOWED=ALTER
```

Figure 33. Listing of Process Records

For Figure 33 on page 122:

Note:

1. Token-related information in the report is extracted from the Type 53 relocate sections. The format of these records is documented in *z/VM: RACF Security Server Macros and Interfaces*.
2. `TOKEN STATUS=(CREATED BY PRE RACF 1.9 CALL)` means that the TOKLT19 bit was set. This bit was set when a token is created and based on a pre-RACF 1.9 ACEE. The bit was on in the UTOKEN that was copied to the SMF record.
3. The following text may appear in the report:

   ```
   **** RECORD TRUNCATED BY RACFRW – INFORMATION LOST ****
   ```

   This indicates that the LRECL value on the SORTIN DD statement was too small or that the value of WRKLRECL (in the ICHRSMFI module) was too small. See “Record Reformatting:” on page 93 for more details.
4. When a profile is not found and *BYPASS* was the user ID on RACHECK, the audit record will have the entity name, not the profile name.

```
2006.196 14:23:38                                RACF REPORT - SHORT USER SUMMARY
                                                 ------------------- R E S O U R C E   S T A T I S T I C S -------------------
   USER/     NAME                 ---- JOB/LOGON ----                          ------------ I N T E N T S ------------
   *JOB                         SUCCESS VIOLATION   SUCCESS   WARNING VIOLATION     ALTER   CONTROL    UPDATE      READ     TOTAL
*CLRMANB                              1         0         0         0         0         0         0         0         0         0
 IBMUSER                              7         0         0         0         0         0         0         0         0         0
 RACUSR1                              0         0         1         0         0         0         0         0         0         1
 RACUSR1    MARY BAILEY               0         0        21         0         0        21         0         0         0        21
 RACUSR2                              0         0         1         0         0         0         0         0         0         1
 RACUSR2    MARY PURCELL              0         0         1         0         0         1         0         0         0         1
 RACUSR3                              0         0         1         0         0         0         0         0         0         1
 RACUSR3    HARRIET BIRD              0         0         1         0         0         1         0         0         0         1
 RACUSR4                              0         0         1         0         0         0         0         0         0         1
 RACUSR4    JOHN H. BUKOWSKI          0         0         1         0         0         1         0         0         0         1
 RACUSR5                              0         0         1         0         0         0         0         0         0         1
 RACUSR5    MELANIE WILKES            0         0         1         0         0         1         0         0         0         1
 RACUSR6                              0         0         1         0         0         0         0         0         0         1
 RACUSR6    FRED PRETOCK              0         0         1         0         0         1         0         0         0         1
 RACUSR7                              0         0         1         0         0         0         0         0         0         1
 RACUSR7    HESTER WILSON             0         0         1         0         0         1         0         0         0         1
 SLCUSRD1                             0         0         1         0         0         0         0         0         1         1
 SLCUSRD5                             0         0         0         0         1         0         0         0         1         1
 ACCUMULATED TOTALS -                 8         0        35         0         1        27         0         0         2        36
 PERCENTAGE OF TOTAL ACCESSES -                       97 %       0 %       3 %      75 %       0 %       0 %       6 %
 UNDEFINED USERS (JOBS) ONLY
 ACCUMULATED TOTALS -                 1         0         0         0         0         0         0         0         0         0
 PERCENTAGE OF TOTAL ACCESSES -                        0 %       0 %       0 %       0 %       0 %       0 %       0 %
```

Figure 34. Short User Summary Report

```
2006.196 14:23:38                                RACF REPORT - SHORT GROUP SUMMARY
                                                 ------------------- R E S O U R C E   S T A T I S T I C S -------------------
  GROUP/                        ---- JOB/LOGON ----                          ------------ I N T E N T S ------------
  *STEP                         SUCCESS VIOLATION   SUCCESS   WARNING VIOLATION     ALTER   CONTROL    UPDATE      READ     TOTAL
**                                    1         0         0         0         0         0         0         0         0         0
 SYS1                                 7         0        35         0         1        27         0         0         2        36
 ACCUMULATED TOTALS -                 8         0        35         0         1        27         0         0         2        36
 PERCENTAGE OF TOTAL ACCESSES -                       97 %       0 %       3 %      75 %       0 %       0 %       6 %
 UNDEFINED USERS (JOBS) ONLY
 ACCUMULATED TOTALS -                 1         0         0         0         0         0         0         0         0         0
 PERCENTAGE OF TOTAL ACCESSES -                        0 %       0 %       0 %       0 %       0 %       0 %       0 %
```

Figure 35. Short Group Summary Report

```
2006.196 14:23:38                               RACF REPORT - SHORT RESOURCE SUMMARY                                  PAGE  13
                                                                                 ------------ I N T E N T S ------------
                RESOURCE NAME                      SUCCESS   WARNING VIOLATION     ALTER   CONTROL    UPDATE      READ     TOTAL
CLASS = DATASET
  RACUSR1.NEW.DS1                                        3         0         0         2         0         0         0         3
  RACUSR2.NEW.DS2                                        3         0         0         2         0         0         0         3
  RACUSR3.NEW.DS3                                        3         0         0         2         0         0         0         3
  RACUSR4.NEW.DS4                                        3         0         0         2         0         0         0         3
  RACUSR5.NEW.DS5                                        3         0         0         2         0         0         0         3
  RACUSR6.NEW.DS6                                        3         0         0         2         0         0         0         3
  RACUSR7.NEW.DS7                                        3         0         0         2         0         0         0         3
  SLCUSRD0.SLCDSND0                                      2         0         0         2         0         0         0         2
  SLCUSRD1.SLCDSND1                                      3         0         0         2         0         0         1         3
  SLCUSRD3.SLCDSND3                                      2         0         0         2         0         0         0         2
  SLCUSRD4.SLCDSND4                                      2         0         0         2         0         0         0         2
  SLCUSRD5.SLCDSND5                                      2         0         1         2         0         0         1         3
CLASS = SECDATA
  SECLEVEL                                               3         0         0         3         0         0         0         3
ACCUMULATED TOTALS -                                    35         0         1        27         0         0         2        36
PERCENTAGE OF TOTAL ACCESSES -                       97 %       0 %       3 %      75 %       0 %       0 %       6 %
GENERIC PROFILE USED
ACCUMULATED TOTALS -                                     0         0         0         0         0         0         0         0
PERCENTAGE OF TOTAL ACCESSES -                        0 %       0 %       0 %       0 %       0 %       0 %       0 %
```

Figure 36. Short Resource Summary Report

```
2007.053 13:51:40                              RACF REPORT - SHORT COMMAND SUMMARY
                     QUALIFIER                 OCCURRENCES
EVENT = 8 - ADDSD COMMAND
            0 - NO VIOLATIONS DETECTED                3
            ACCUMULATED TOTALS -                      3
EVENT = 9 - ADDGROUP COMMAND
            0 - NO VIOLATIONS DETECTED                1
            ACCUMULATED TOTALS -                      1
EVENT = 10 - ADDUSER COMMAND
            0 - NO VIOLATIONS DETECTED                7
            ACCUMULATED TOTALS -                      7
EVENT = 13 - ALTUSER COMMAND
            0 - NO VIOLATIONS DETECTED                1
            ACCUMULATED TOTALS -                      1
EVENT = 14 - CONNECT COMMAND
            0 - NO VIOLATIONS DETECTED                1
            ACCUMULATED TOTALS                        1
EVENT = 15 - DELDSD COMMAND
            0 - NO VIOLATIONS DETECTED                2
            ACCUMULATED TOTALS -                      2
EVENT = 16 - DELGROUP COMMAND
            0 - NO VIOLATIONS DETECTED                1
            ACCUMULATED TOTALS -                      1
EVENT = 17 - DELUSER COMMAND
            0 - NO VIOLATIONS DETECTED                1
            ACCUMULATED TOTALS -                      1
EVENT = 19 - PERMIT COMMAND
            0 - NO VIOLATIONS DETECTED               14
            ACCUMULATED TOTALS                       14
EVENT = 20 - RALTER COMMAND
            0 - NO VIOLATIONS DETECTED                2
            ACCUMULATED TOTALS -                      2
EVENT = 21 - RDEFINE COMMAND
            0 - NO VIOLATIONS DETECTED                7
            ACCUMULATED TOTALS -                      7
EVENT = 22 - RDELETE COMMAND
            0 - NO VIOLATIONS DETECTED                7
            ACCUMULATED TOTALS -                      7
EVENT = 23 - REMOVE COMMAND
            0 - NO VIOLATIONS DETECTED                1
            ACCUMULATED TOTALS                        1
EVENT = 24 - SETROPTS COMMAND
            0 - NO VIOLATIONS DETECTED               49
            ACCUMULATED TOTALS -                     49
```

Figure 37. Short Command Summary Report

```
2007.053 13:51:40                               RACF REPORT - SHORT EVENT SUMMARY
                     QUALIFIER                 OCCURRENCES
EVENT = 1 - JOB INITIATION / TSO LOGON
            0 - SUCCESSFUL INITIATION/LOGON         4
            1 - INVALID PASSWORD                    1
            8 - SUCCESSFUL TERMINATION              5
            10-INSUFF. SECURITY LABEL AUTHORITY     4
            11-NOT AUTHORIZED TO SECURITY LABEL     3
            18-SUBMITTER UNAUTHOR. TO SEC. LABEL    1
            26-INVALID NEW PASSWORD                 1
            ACCUMULATED TOTALS -                   19
EVENT = 2 - RESOURCE ACCESS
            0 - SUCCESSFUL ACCESS                   9
            1 - INSUFFICIENT AUTHORITY              1
            ACCUMULATED TOTALS -                   10
EVENT = 8 - ADDSD COMMAND
            0 - NO VIOLATIONS DETECTED              3
            ACCUMULATED TOTALS -                    3
EVENT = 9 - ADDGROUP COMMAND
            0 - NO VIOLATIONS DETECTED              1
            ACCUMULATED TOTALS -                    1
EVENT = 10 - ADDUSER COMMAND
            0 - NO VIOLATIONS DETECTED              7
            ACCUMULATED TOTALS -                    7
EVENT = 13 - ALTUSER COMMAND
            0 - NO VIOLATIONS DETECTED              1
            ACCUMULATED TOTALS -                    1
EVENT = 14 - CONNECT COMMAND
            0 - NO VIOLATIONS DETECTED              1
            ACCUMULATED TOTALS -                    1
EVENT = 15 - DELDSD COMMAND
            0 - NO VIOLATIONS DETECTED              2
            ACCUMULATED TOTALS -                    2
EVENT = 16 - DELGROUP COMMAND
            0 - NO VIOLATIONS DETECTED              1
            ACCUMULATED TOTALS                      1
EVENT = 17 - DELUSER COMMAND
            0 - NO VIOLATIONS DETECTED              1
            ACCUMULATED TOTALS -                    1
EVENT = 19 - PERMIT COMMAND
            0 - NO VIOLATIONS DETECTED             14
            ACCUMULATED TOTALS -                   14
EVENT = 20 - RALTER COMMAND
            0 - NO VIOLATIONS DETECTED              2
            ACCUMULATED TOTALS -                    2
EVENT = 21 - RDEFINE COMMAND
            0 - NO VIOLATIONS DETECTED              7
            ACCUMULATED TOTALS -                    7
EVENT = 22 - RDELETE COMMAND
            0 - NO VIOLATIONS DETECTED              7
            ACCUMULATED TOTALS -                    7
EVENT = 23 - REMOVE COMMAND
            0 - NO VIOLATIONS DETECTED              1
            ACCUMULATED TOTALS -                    1
EVENT = 24 - SETROPTS COMMAND
            0 - NO VIOLATIONS DETECTED             49
            ACCUMULATED TOTALS -                   49
        ACCUMULATED TOTALS -                      126
```

Figure 38. Short Event Summary Report

```
2006.196 14:23:38                    RACF REPORT - SHORT OWNER SUMMARY
                                                  ------------ I N T E N T S ------------
    OWNER                             SUCCESS   WARNING VIOLATION     ALTER   CONTROL    UPDATE      READ     TOTAL
 RACUSR1                                    6         0         0         5         0         0         0         6
 RACUSR2                                    3         0         0         2         0         0         0         3
 RACUSR3                                    3         0         0         2         0         0         0         3
 RACUSR4                                    3         0         0         2         0         0         0         3
 RACUSR5                                    3         0         0         2         0         0         0         3
 RACUSR6                                    3         0         0         2         0         0         0         3
 RACUSR7                                    3         0         0         2         0         0         0         3
 SLCUSRD0                                   2         0         0         2         0         0         0         2
 SLCUSRD1                                   3         0         0         2         0         0         1         3
 SLCUSRD3                                   2         0         0         2         0         0         0         2
 SLCUSRD4                                   2         0         0         2         0         0         0         2
 SLCUSRD5                                   2         0         1         2         0         0         1         3
 ACCUMULATED TOTALS -                      35         0         1        27         0         0         2        36
 PERCENTAGE OF TOTAL ACCESSES -            97 %       0 %       3 %      75 %       0 %       0 %       6 %
```

Figure 39. Short Owner Summary Report

```
2006.218 12:36:12                    RACF REPORT - USER BY RESOURCE SUMMARY
                                                  ------------ I N T E N T S ------------
                  RESOURCE NAME       SUCCESS   WARNING VIOLATION     ALTER   CONTROL    UPDATE      READ     TOTAL
USER =  IBMUSER
  NAME =     JOHN P. ZILLER
  CLASS = SECDATA
    SECLEVEL                                1         0         0         1         0         0         0         1
  ACCUMULATED TOTALS -                      1         0         0         1         0         0         0         1
  PERCENTAGE OF TOTAL ACCESSES -          100 %       0 %       0 %     100 %       0 %       0 %       0 %
  GENERIC PROFILE USED
  ACCUMULATED TOTALS -                      0         0         0         0         0         0         0         0
  PERCENTAGE OF TOTAL ACCESSES -            0 %       0 %       0 %       0 %       0 %       0 %       0 %
USER =  RACUSR1
  CLASS = DATASET
    RACUSR1.NEW.DS1                         0         0         0         0         0         0         0         0
  NAME =     MARY BAILEY
  CLASS = DATASET
    RACUSR1.NEW.DS1                         2         0         0         1         0         0         0         2
    RACUSR1.SMFS23                          2         0         0         2         0         0         0         2
  NAME =     MARY BAILEY
  CLASS = SECDATA
    SECLEVEL                                5         0         0         5         0         0         0         5
  ACCUMULATED TOTALS -                      9         0         0         8         0         0         0         9
  PERCENTAGE OF TOTAL ACCESSES -          100 %       0 %       0 %      89 %       0 %       0 %       0 %
  GENERIC PROFILE USED
  ACCUMULATED TOTALS -                      0         0         0         0         0         0         0         0
  PERCENTAGE OF TOTAL ACCESSES -            0 %       0 %       0 %       0 %       0 %       0 %       0 %
USER =  RACUSR2
  CLASS = DATASET
    RACUSR2.NEW.DS2                         0         0         0         0         0         0         0         0
  NAME =     JOHN P. ZILLER
  CLASS = DATASET
    RACUSR2.NEW.DS2                         2         0         0         1         0         0         0         2
  ACCUMULATED TOTALS -                      2         0         0         1         0         0         0         2
  PERCENTAGE OF TOTAL ACCESSES -          100 %       0 %       0 %      50 %       0 %       0 %       0 %
  GENERIC PROFILE USED
  ACCUMULATED TOTALS -                      0         0         0         0         0         0         0         0
  PERCENTAGE OF TOTAL ACCESSES -            0 %       0 %       0 %       0 %       0 %       0 %       0 %
USER =  RACUSR3
  CLASS = DATASET
```

Figure 40. User by Resource Summary Report

```
2006.218 12:36:12                    RACF REPORT - GROUP BY RESOURCE SUMMARY
                                                  ------------ I N T E N T S ------------
                  RESOURCE NAME       SUCCESS   WARNING VIOLATION     ALTER   CONTROL    UPDATE      READ     TOTAL
GROUP =  SYS1
  CLASS = DATASET
    RACUSR1.NEW.DS1                         2         0         0         1         0         0         0         2
    RACUSR1.SMFS23                          2         0         0         2         0         0         0         2
    RACUSR2.NEW.DS2                         2         0         0         1         0         0         0         2
    RACUSR3.NEW.DS3                         2         0         0         1         0         0         0         2
    RACUSR4.NEW.DS4                         2         0         0         1         0         0         0         2
    RACUSR5.NEW.DS5                         2         0         0         1         0         0         0         2
    RACUSR6.NEW.DS6                         2         0         0         1         0         0         0         2
    SLCUSRD1.SLCDSND1                       2         0         0         0         0         0         2         2
    SLCUSRD3.SLCDSND3                       1         0         0         0         0         0         1         1
    SLCUSRD5.SLCDSND5                       0         0         2         0         0         0         2         2
  CLASS = SECDATA
    SECLEVEL                                6         0         0         6         0         0         0         6
  ACCUMULATED TOTALS -                     23         0         2        14         0         0         5        25
  PERCENTAGE OF TOTAL ACCESSES -           92 %       0 %       8 %      56 %       0 %       0 %      20 %
  GENERIC PROFILE USED
  ACCUMULATED TOTALS -                      0         0         0         0         0         0         0         0
  PERCENTAGE OF TOTAL ACCESSES -            0 %       0 %       0 %       0 %       0 %       0 %       0 %
```

Figure 41. Group by Resource Summary Report

```
2006.218 12:36:12                       RACF REPORT - RESOURCE BY USER SUMMARY
      USER/                                                 ------------ I N T E N T S ------------
      *JOB                                 SUCCESS   WARNING VIOLATION     ALTER   CONTROL    UPDATE      READ     TOTAL
DATASET = RACUSR1.NEW.DS1
    RACUSR1    MARY BAILEY                     2         0         0         1         0         0         0         2
    ACCUMULATED TOTALS -                       2         0         0         1         0         0         0         2
    PERCENTAGE OF TOTAL ACCESSES -           100 %       0 %       0 %      50 %       0 %       0 %       0 %
    UNDEFINED USERS (JOBS) ONLY
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
    PERCENTAGE OF TOTAL ACCESSES -             0 %       0 %       0 %       0 %       0 %       0 %       0 %
    GENERIC PROFILE USED
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
    PERCENTAGE OF TOTAL ACCESSES -             0 %       0 %       0 %       0 %       0 %       0 %       0 %
DATASET = RACUSR1.SMFS23
    RACUSR1    MARY BAILEY                     2         0         0         2         0         0         0         2
    ACCUMULATED TOTALS -                       2         0         0         2         0         0         0         2
    PERCENTAGE OF TOTAL ACCESSES -           100 %       0 %       0 %     100 %       0 %       0 %       0 %
    UNDEFINED USERS (JOBS) ONLY
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
    PERCENTAGE OF TOTAL ACCESSES -             0 %       0 %       0 %       0 %       0 %       0 %       0 %
    GENERIC PROFILE USED
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
    PERCENTAGE OF TOTAL ACCESSES -             0 %       0 %       0 %       0 %       0 %       0 %       0 %
DATASET = RACUSR2.NEW.DS2
    RACUSR2    JOHN P. ZILLER                  2         0         0         1         0         0         0         2
    ACCUMULATED TOTALS -                       2         0         0         1         0         0         0         2
    PERCENTAGE OF TOTAL ACCESSES -           100 %       0 %       0 %      50 %       0 %       0 %       0 %
    UNDEFINED USERS (JOBS) ONLY
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
    PERCENTAGE OF TOTAL ACCESSES -             0 %       0 %       0 %       0 %       0 %       0 %       0 %
    GENERIC PROFILE USED
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
    PERCENTAGE OF TOTAL ACCESSES -             0 %       0 %       0 %       0 %       0 %       0 %       0 %
DATASET = RACUSR3.NEW.DS3
    RACUSR3    HARRIET BIRD                    2         0         0         1         0         0         0         2
    ACCUMULATED TOTALS -                       2         0         0         1         0         0         0         2
    PERCENTAGE OF TOTAL ACCESSES -           100 %       0 %       0 %      50 %       0 %       0 %       0 %
    UNDEFINED USERS (JOBS) ONLY
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
    PERCENTAGE OF TOTAL ACCESSES -             0 %       0 %       0 %       0 %       0 %       0 %       0 %
    GENERIC PROFILE USED
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
    PERCENTAGE OF TOTAL ACCESSES -             0 %       0 %       0 %       0 %       0 %       0 %       0 %
DATASET = RACUSR4.NEW.DS4
    RACUSR4    JOHN H. BUKOWSKI                2         0         0         1         0         0         0         2
    ACCUMULATED TOTALS -                       2         0         0         1         0         0         0         2
    PERCENTAGE OF TOTAL ACCESSES -           100 %       0 %       0 %      50 %       0 %       0 %       0 %
    UNDEFINED USERS (JOBS) ONLY
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
```

Figure 42. Resource by User Summary Report

```
2006.218 12:36:12                       RACF REPORT - RESOURCE BY GROUP SUMMARY
    GROUP/                                              ------------ I N T E N T S ------------
    *STEP                                  SUCCESS   WARNING VIOLATION     ALTER   CONTROL    UPDATE      READ     TOTAL
DATASET = RACUSR1.NEW.DS1
    SYS1                                       2         0         0         1         0         0         0         2
    ACCUMULATED TOTALS -                       2         0         0         1         0         0         0         2
    PERCENTAGE OF TOTAL ACCESSES -           100 %       0 %       0 %      50 %       0 %       0 %       0 %
    UNDEFINED USERS (JOBS) ONLY
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
    PERCENTAGE OF TOTAL ACCESSES -             0 %       0 %       0 %       0 %       0 %       0 %       0 %
    GENERIC PROFILE USED
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
    PERCENTAGE OF TOTAL ACCESSES -             0 %       0 %       0 %       0 %       0 %       0 %       0 %
DATASET = RACUSR1.SMFS23
    SYS1                                       2         0         0         2         0         0         0         2
    ACCUMULATED TOTALS -                       2         0         0         2         0         0         0         2
    PERCENTAGE OF TOTAL ACCESSES -           100 %       0 %       0 %     100 %       0 %       0 %       0 %
    UNDEFINED USERS (JOBS) ONLY
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
    PERCENTAGE OF TOTAL ACCESSES -             0 %       0 %       0 %       0 %       0 %       0 %       0 %
    GENERIC PROFILE USED
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
    PERCENTAGE OF TOTAL ACCESSES -             0 %       0 %       0 %       0 %       0 %       0 %       0 %
DATASET = RACUSR2.NEW.DS2
    SYS1                                       2         0         0         1         0         0         0         2
    ACCUMULATED TOTALS -                       2         0         0         1         0         0         0         2
    PERCENTAGE OF TOTAL ACCESSES -           100 %       0 %       0 %      50 %       0 %       0 %       0 %
    UNDEFINED USERS (JOBS) ONLY
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
    PERCENTAGE OF TOTAL ACCESSES -             0 %       0 %       0 %       0 %       0 %       0 %       0 %
    GENERIC PROFILE USED
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
    PERCENTAGE OF TOTAL ACCESSES -             0 %       0 %       0 %       0 %       0 %       0 %       0 %
DATASET = RACUSR3.NEW.DS3
    SYS1                                       2         0         0         1         0         0         0         2
    ACCUMULATED TOTALS -                       2         0         0         1         0         0         0         2
    PERCENTAGE OF TOTAL ACCESSES -           100 %       0 %       0 %      50 %       0 %       0 %       0 %
    UNDEFINED USERS (JOBS) ONLY
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
    PERCENTAGE OF TOTAL ACCESSES -             0 %       0 %       0 %       0 %       0 %       0 %       0 %
    GENERIC PROFILE USED
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
    PERCENTAGE OF TOTAL ACCESSES -             0 %       0 %       0 %       0 %       0 %       0 %       0 %
DATASET = RACUSR4.NEW.DS4
    SYS1                                       2         0         0         1         0         0         0         2
    ACCUMULATED TOTALS -                       2         0         0         1         0         0         0         2
    PERCENTAGE OF TOTAL ACCESSES -           100 %       0 %       0 %      50 %       0 %       0 %       0 %
    UNDEFINED USERS (JOBS) ONLY
    ACCUMULATED TOTALS -                       0         0         0         0         0         0         0         0
```

Figure 43. Resource by Group Summary Report

```
2006.218 12:36:12                          RACF REPORT - RESOURCE BY EVENT SUMMARY
              EVENT/QUALIFIER                OCCURRENCES
DATASET = RACUSR1.NEW.DS1
        7 - DEFINE RESOURCE
            0 - SUCCESSFUL DEFINITION                  1
            ACCUMULATED TOTALS -                       1
            GENERIC PROFILE USED
            ACCUMULATED TOTALS -                       0
        8 - ADDSD COMMAND
            0 - NO VIOLATIONS DETECTED                 1
            ACCUMULATED TOTALS -                       1
            GENERIC PROFILE USED
            ACCUMULATED TOTALS -                       0
        ACCUMULATED TOTALS -                           2
        GENERIC PROFILE USED
        ACCUMULATED TOTALS -                           0
DATASET = RACUSR1.SMFS23
        8 - ADDSD COMMAND
            0 - NO VIOLATIONS DETECTED                 1
            ACCUMULATED TOTALS -                       1
            GENERIC PROFILE USED
            ACCUMULATED TOTALS -                       0
        19 - PERMIT COMMAND
            0 - NO VIOLATIONS DETECTED                 1
            ACCUMULATED TOTALS -                       1
            GENERIC PROFILE USED
            ACCUMULATED TOTALS -                       0
        ACCUMULATED TOTALS -                           2
        GENERIC PROFILE USED
        ACCUMULATED TOTALS -                           0
DATASET = RACUSR2.NEW.DS2
        7 - DEFINE RESOURCE
            0 - SUCCESSFUL DEFINITION                  1
            ACCUMULATED TOTALS -                       1
            GENERIC PROFILE USED
            ACCUMULATED TOTALS -                       0
        8 - ADDSD COMMAND
            0 - NO VIOLATIONS DETECTED                 1
            ACCUMULATED TOTALS -                       1
            GENERIC PROFILE USED
            ACCUMULATED TOTALS -                       0
```

Figure 44. Resource by Event Summary Report

```
2006.218 12:36:12                          RACF REPORT - EVENT BY RESOURCE SUMMARY
                     QUALIFIER               OCCURRENCES    RESOURCE
EVENT = 2 - RESOURCE ACCESS
            0 - SUCCESSFUL ACCESS
                                                       2      DATASET  = SLCUSRD1.SLCDSND1
                                                       1      DATASET  = SLCUSRD3.SLCDSND3
                ACCUMULATED TOTALS -                   3
                GENERIC PROFILE USED
                ACCUMULATED TOTALS -                   0
                UNKNOWN EVENT CODE QUALIFIER
                                                       2      DATASET  = SLCUSRD5.SLCDSND5
                ACCUMULATED TOTALS -                   2
                GENERIC PROFILE USED
                ACCUMULATED TOTALS -                   0
            ACCUMULATED TOTALS -                       5
            GENERIC PROFILE USED
            ACCUMULATED TOTALS -                       0
EVENT = 7 - DEFINE RESOURCE
            0 - SUCCESSFUL DEFINITION
                                                       1      DATASET  = RACUSR1.NEW.DS1
                                                       1      DATASET  = RACUSR2.NEW.DS2
                                                       1      DATASET  = RACUSR3.NEW.DS3
                                                       1      DATASET  = RACUSR4.NEW.DS4
                                                       1      DATASET  = RACUSR5.NEW.DS5
                                                       1      DATASET  = RACUSR6.NEW.DS6
                ACCUMULATED TOTALS -                   6
                GENERIC PROFILE USED
                ACCUMULATED TOTALS -                   0
            ACCUMULATED TOTALS -                       6
            GENERIC PROFILE USED
            ACCUMULATED TOTALS -                       0
EVENT = 8 - ADDSD COMMAND
            0 - NO VIOLATIONS DETECTED
                                                       1      DATASET  = RACUSR1.NEW.DS1
                                                       1      DATASET  = RACUSR1.SMFS23
                                                       1      DATASET  = RACUSR2.NEW.DS2
                                                       1      DATASET  = RACUSR3.NEW.DS3
                                                       1      DATASET  = RACUSR4.NEW.DS4
                                                       1      DATASET  = RACUSR5.NEW.DS5
                                                       1      DATASET  = RACUSR6.NEW.DS6
                ACCUMULATED TOTALS -                   7
                GENERIC PROFILE USED
                ACCUMULATED TOTALS -                   0
            ACCUMULATED TOTALS -                       7
            GENERIC PROFILE USED
```

Figure 45. Event by Resource Summary Report

```
2006.218 12:36:12                          RACF REPORT - COMMAND BY USER SUMMARY
                  QUALIFIER                 OCCURRENCES    USER         NAME
EVENT = 8 - ADDSD COMMAND
          0 - NO VIOLATIONS DETECTED
                                                      2      RACUSR1    MARY BAILEY
                                                      1      RACUSR2    JOHN P. ZILLER
                                                      1      RACUSR3    HARRIET BIRD
                                                      1      RACUSR4    JOHN H. BUKOWSKI
                                                      1      RACUSR5    MELANIE WILKES
                                                      1      RACUSR6
              ACCUMULATED TOTALS -                    7
          ACCUMULATED TOTALS -                        7
EVENT = 10 - ADDUSER COMMAND
          0 - NO VIOLATIONS DETECTED
                                                      0      IBMUSER
                                                      1      IBMUSER    THOR
                                                      6      RACUSR1    MARY BAILEY
              ACCUMULATED TOTALS -                    7
          1 - INSUFFICIENT AUTHORITY
                                                      1      RACUSR7    HESTER WILSON
                                                      2      SLCUSRD0       (NAME UNKNOWN)
                                                      2      SLCUSRD1       (NAME UNKNOWN)
                                                      2      SLCUSRD3       (NAME UNKNOWN)
                                                      2      SLCUSRD4       (NAME UNKNOWN)
                                                      2      SLCUSRD5       (NAME UNKNOWN)
                                                      2      SLCUSRD6       (NAME UNKNOWN)
              ACCUMULATED TOTALS -                   13
          ACCUMULATED TOTALS -                       20
EVENT = 13 - ALTUSER COMMAND
          0 - NO VIOLATIONS DETECTED
                                                      0      IBMUSER
                                                      1      IBMUSER    THOR
                                                     21      RACUSR1    MARY BAILEY
              ACCUMULATED TOTALS -                   22
          ACCUMULATED TOTALS -                       22
EVENT = 17 - DELUSER COMMAND
          0 - NO VIOLATIONS DETECTED
                                                      0      IBMUSER
                                                      1      IBMUSER    THOR
              ACCUMULATED TOTALS -                    1
          ACCUMULATED TOTALS -                        1
```

Figure 46. Command by User Summary Report

```
2006.218 12:36:12                          RACF REPORT - COMMAND BY GROUP SUMMARY
                  QUALIFIER                 OCCURRENCES    GROUP
EVENT = 8 - ADDSD COMMAND
          0 - NO VIOLATIONS DETECTED
                                                      7      SYS1
              ACCUMULATED TOTALS -                    7
          ACCUMULATED TOTALS -                        7
EVENT = 10 - ADDUSER COMMAND
          0 - NO VIOLATIONS DETECTED
                                                      7      SYS1
              ACCUMULATED TOTALS -                    7
          1 - INSUFFICIENT AUTHORITY
                                                     13      SYS1
              ACCUMULATED TOTALS -                   13
          ACCUMULATED TOTALS -                       20
EVENT = 13 - ALTUSER COMMAND
          0 - NO VIOLATIONS DETECTED
                                                     22      SYS1
              ACCUMULATED TOTALS -                   22
          ACCUMULATED TOTALS -                       22
EVENT = 17 - DELUSER COMMAND
          0 - NO VIOLATIONS DETECTED
                                                      1      SYS1
              ACCUMULATED TOTALS -                    1
          ACCUMULATED TOTALS -                        1
EVENT = 19 - PERMIT COMMAND
          0 - NO VIOLATIONS DETECTED
                                                      1      SYS1
              ACCUMULATED TOTALS -                    1
          ACCUMULATED TOTALS -                        1
EVENT = 20 - RALTER COMMAND
          0 - NO VIOLATIONS DETECTED
                                                      1      SYS1
              ACCUMULATED TOTALS -                    1
```

Figure 47. Command by Group Summary Report

```
2006.218 12:36:12                          RACF REPORT - COMMAND BY RESOURCE SUMMARY
                    QUALIFIER                 OCCURRENCES    RESOURCE
EVENT = 8 - ADDSD COMMAND
            0 - NO VIOLATIONS DETECTED
                                                        1      DATASET  = RACUSR1.NEW.DS1
                                                        1      DATASET  = RACUSR1.SMFS23
                                                        1      DATASET  = RACUSR2.NEW.DS2
                                                        1      DATASET  = RACUSR3.NEW.DS3
                                                        1      DATASET  = RACUSR4.NEW.DS4
                                                        1      DATASET  = RACUSR5.NEW.DS5
                                                        1      DATASET  = RACUSR6.NEW.DS6
                ACCUMULATED TOTALS -                    7
                GENERIC PROFILE USED
                ACCUMULATED TOTALS -                    0
            ACCUMULATED TOTALS -                        7
            GENERIC PROFILE USED
            ACCUMULATED TOTALS -                        0
EVENT = 19 - PERMIT COMMAND
            0 - NO VIOLATIONS DETECTED
                                                        1      DATASET  = RACUSR1.SMFS23
                ACCUMULATED TOTALS -                    1
                GENERIC PROFILE USED
                ACCUMULATED TOTALS -                    0
            ACCUMULATED TOTALS -                        1
            GENERIC PROFILE USED
            ACCUMULATED TOTALS -                        0
EVENT = 20 - RALTER COMMAND
            0 - NO VIOLATIONS DETECTED
                                                        1      SECDATA  = SECLEVEL
                ACCUMULATED TOTALS -                    1
                GENERIC PROFILE USED
                ACCUMULATED TOTALS -                    0
            ACCUMULATED TOTALS -                        1
            GENERIC PROFILE USED
            ACCUMULATED TOTALS -                        0
EVENT = 21 - RDEFINE COMMAND
            0 - NO VIOLATIONS DETECTED
                                                        3      SECDATA  = SECLEVEL
                ACCUMULATED TOTALS -                    3
                GENERIC PROFILE USED
                ACCUMULATED TOTALS -                    0
            ACCUMULATED TOTALS -                        3
            GENERIC PROFILE USED
```

Figure 48. Command by Resource Summary Report

```
2006.218 12:36:12                          RACF REPORT - OWNER BY RESOURCE SUMMARY
                                                        ------------ I N T E N T S ------------
                RESOURCE NAME               SUCCESS   WARNING VIOLATION     ALTER   CONTROL    UPDATE      READ     TOTAL
OWNER =  IBMUSER
  CLASS = SECDATA
    SECLEVEL                                      1         0         0         1         0         0         0         1
  ACCUMULATED TOTALS -                            1         0         0         1         0         0         0         1
  PERCENTAGE OF TOTAL ACCESSES -                100 %       0 %       0 %     100 %       0 %       0 %       0 %
  GENERIC PROFILE USED
  ACCUMULATED TOTALS -                            0         0         0         0         0         0         0         0
  PERCENTAGE OF TOTAL ACCESSES -                  0 %       0 %       0 %       0 %       0 %       0 %       0 %
OWNER =  RACUSR1
  CLASS = DATASET
    RACUSR1.NEW.DS1                               2         0         0         1         0         0         0         2
    RACUSR1.SMFS23                                2         0         0         2         0         0         0         2
  CLASS = SECDATA
    SECLEVEL                                      5         0         0         5         0         0         0         5
  ACCUMULATED TOTALS -                            9         0         0         8         0         0         0         9
  PERCENTAGE OF TOTAL ACCESSES -                100 %       0 %       0 %      89 %       0 %       0 %       0 %
  GENERIC PROFILE USED
  ACCUMULATED TOTALS -                            0         0         0         0         0         0         0         0
  PERCENTAGE OF TOTAL ACCESSES -                  0 %       0 %       0 %       0 %       0 %       0 %       0 %
OWNER =  RACUSR2
  CLASS = DATASET
    RACUSR2.NEW.DS2                               2         0         0         1         0         0         0         2
  ACCUMULATED TOTALS -                            2         0         0         1         0         0         0         2
  PERCENTAGE OF TOTAL ACCESSES -                100 %       0 %       0 %      50 %       0 %       0 %       0 %
  GENERIC PROFILE USED
  ACCUMULATED TOTALS -                            0         0         0         0         0         0         0         0
  PERCENTAGE OF TOTAL ACCESSES -                  0 %       0 %       0 %       0 %       0 %       0 %       0 %
OWNER =  RACUSR3
  CLASS = DATASET
    RACUSR3.NEW.DS3                               2         0         0         1         0         0         0         2
  ACCUMULATED TOTALS -                            2         0         0         1         0         0         0         2
  PERCENTAGE OF TOTAL ACCESSES -                100 %       0 %       0 %      50 %       0 %       0 %       0 %
  GENERIC PROFILE USED
  ACCUMULATED TOTALS -                            0         0         0         0         0         0         0         0
  PERCENTAGE OF TOTAL ACCESSES -                  0 %       0 %       0 %       0 %       0 %       0 %       0 %
OWNER =  RACUSR4
  CLASS = DATASET
    RACUSR4.NEW.DS4                               2         0         0         1         0         0         0         2
  ACCUMULATED TOTALS -                            2         0         0         1         0         0         0         2
  PERCENTAGE OF TOTAL ACCESSES -                100 %       0 %       0 %      50 %       0 %       0 %       0 %
```

Figure 49. Owner by Resource Summary Report

Sample Report Writer Output for Shared User IDs

Shared ID Sample Report 1

In this sample report, CHIEF logs on successfully to DirMaint and attempts to link to RACFVM's 305, for which DirMaint is not authorized.

```
2006.293 16:13:28                              RACF REPORT - LISTING OF PROCESS RECORDS
                                                          E
                                                          V  Q
                                                          E  U
                      *JOB/USER  *STEP/    --TERMINAL--  N  A
 DATE    TIME   SYSID   NAME     GROUP       ID    LVL  T  L
2006.293 16:06:26 VMSP  DIRMAINT  SYS1    LOGN0322   0  1 12  JOBID=( 00.000 00:00:00),USERDATA=()
                      DIRMAINT MACHINE                        AUTH=(NONE),REASON=(NONE)
                                                              LOGSTR='LOGON BY',
                                                              SESSION=TSO LOGON,TOKEN USER ATTRIBUTES=(SURROGATE USERID),TERMINAL=
                                                              LOGN0322,SUBMITTING USER=CHIEF,SUBMITTING GROUP=CELTICS
2006.293 16:06:35 VMSP   DIRMAINT  SYS1     LOGN0322   0  2  1  JOBID=( 00.000 00:00:00),USERDATA=(),OWNER=OPERATOR
                      DIRMAINT MACHINE                        AUTH=(NORMAL),REASON=(ENTITY OR FAILSOFT PROCESSING)
                                                              SESSION=TSO LOGON,TOKEN USER ATTRIBUTES=(SURROGATE USERID),TERMINAL=
                                                              LOGN0322,SUBMITTING USER=CHIEF,SUBMITTING GROUP=CELTICS
                                                              VMMDISK=RACFVM.305,LEVEL=00,INTENT=READ,ALLOWED=NONE
```

Figure 50. Shared ID Sample Report 1

Shared ID Sample Report 2

In this sample report, BILL attempts unsuccessfully to logon to DirMaint, for which BILL is not authorized.

```
2006.293 16:11:36                              RACF REPORT - LISTING OF PROCESS RECORDS
                                                          E
                                                          V  Q
                                                          E  U
                      *JOB/USER  *STEP/    --TERMINAL--  N  A
 DATE    TIME   SYSID   NAME     GROUP       ID    LVL  T  L
2006.293 16:07:10 VMSP  DIRMAINT  SYS1    LOGN0322   0  1 17  JOBID=( 00.000 00:00:00),USERDATA=()
                      DIRMAINT MACHINE                        AUTH=(NONE),REASON=(RACINIT FAILURE)
                                                              LOGSTR='LOGON BY',
                                                              SESSION=TSO LOGON,TOKEN USER ATTRIBUTES=(SURROGATE USERID),TERMINAL=
                                                              LOGN0322,SUBMITTING USER=BILL,SUBMITTING GROUP=PISTONS
```

Figure 51. Shared ID Sample Report 2

Shared ID Sample Report 3

In this sample report, the DirMaint user ID is being logged onto directly, which is not allowed. The first record shows the successful verification of DirMaint, followed by an unsuccessful access attempt to the LOGONBY.DIRMAINT SURROGAT profile by DirMaint.

```
2006.293 16:09:47                                 RACF REPORT - LISTING OF PROCESS RECORDS
                                                             E
                                                             V  Q
                                                             E  U
                         *JOB/USER  *STEP/    --TERMINAL--  N  A
 DATE    TIME   SYSID      NAME     GROUP       ID    LVL  T  L
2006.293 16:08:02 VMSP  DIRMAINT  SYS1    LOGN0322   0  1 12  JOBID=( 00.000 00:00:00),USERDATA=()
                      DIRMAINT MACHINE                        AUTH=(NONE),REASON=(NONE)
                                                              LOGSTR='LOGON',
                                                              SESSION=TSO LOGON,TERMINAL=LOGN0322
2006.293 16:08:02 VMSP  DIRMAINT  SYS1    LOGN0322   0  2  1  JOBID=( 00.000 00:00:00),USERDATA=(),OWNER=OPERATOR
                      DIRMAINT MACHINE                        AUTH=(NORMAL),REASON=(ENTITY OR FAILSOFT PROCESSING)
                                                              SESSION=TSO LOGON,TERMINAL=LOGN0322
                                                              SURROGAT=LOGONBY.DIRMAINT,LEVEL=00,INTENT=READ,ALLOWED=NONE
```

Figure 52. Shared ID Sample Report 3

Sample RACFRW CONTROL Files

The following are examples of RACFRW CONTROL files that produce various reports from the RACF report writer.

- This file produces a report with all RACF SMF records sorted by user, and a general summary report showing overall RACF-related system activity. (This report may be large. It can produce more than 10,000 lines.)

```
RACFRW  TITLE ('ALL ACTIVITIES REPORT BY USER') GENSUM
 LIST SORT(USER)
END
```

- This file produces a report of failures to access all RACF protected resources and of violations at logon. A summary report by resource and by user is provided.

```
RACFRW  TITLE ('MONITORING ACCESS VIOLATIONS')
 SELECT PROCESS VIOLATIONS
  EVENT ACCESS EVQUAL(1)
  EVENT LOGON
 LIST SORT(USER  CLASS)
 SUMMARY RESOURCE BY(USER)
 SUMMARY USER BY(RESOURCE)
END
```

- This file produces a summary report of minidisk access violations. The report is sorted by user.

```
RACFRW GENSUM TITLE('ACCESS VIOLATIONS SORTED BY USERID OF OFFENDERS')
 SELECT PROCESS VIOLATIONS
  EVENT ACCESS CLASS(VMMDISK)
 SUMMARY RESOURCE BY(USER)
END
```

- This file produces a report of the activities of SPECIAL and group-SPECIAL users.

```
RACFRW  TITLE ('USERS WITH SPECIAL OR GROUP-SPECIAL ATTRIBUTE REPORT')
 SELECT PROCESS REASON(SPECIAL)
 SELECT PROCESS AUTHORITY(SPECIAL)
  EVENT ALLSVC
  EVENT ALLCOMMAND
LIST SORT(USER)
END
```

- This file produces a list of all the RACF commands issued. The report is sorted by user.

```
RACFRW  TITLE ('MONITORING THE USE OF RACF COMMANDS')
 SELECT PROCESS
  EVENT ALLCOMMAND
 SUMMARY COMMAND BY (USER)
END
```

- This file produces a report of the activities of OPERATIONS and group-OPERATIONS users.

```
RACFRW TITLE('USERS WITH OPERATIONS OR GROUP-OPERATIONS ATTRIBUTE' )
 SELECT PROCESS AUTHORITY(OPERATIONS)
  EVENT ALLSVC
  EVENT ALLCOMMAND
LIST SORT(USER)
END
```

- This file produces a report of password violations at logon.

```
RACFRW  TITLE ('PASSWORD VIOLATION REPORT')
 SELECT PROCESS
  EVENT LOGON EVQUAL(1)
LIST SORT(USER)
END
```

- This file produces a report of failed logons for user Smith.

```
RACFRW TITLE('REPORT ON FAILED LOGONS FOR USER SMITH')
 SELECT PROCESS  USER(DUMMY)
  EVENT LOGON
SUMMARY USER NEWPAGE
END
```

- This file produces a report of access granted only because the warning mode is active.

```
RACFRW  TITLE ('MONITORING ACCESS ATTEMPTS IN WARNING MODE')
 SELECT PROCESS  WARNING
LIST SORT(DATE USER EVENT NAME CLASS)
END
```

- This file produces a report of ALTUSER commands issued by user Jones.

```
RACFRW TITLE('ALTUSER COMMANDS ISSUED BY USER JONES')
 SELECT PROCESS USER(JONES)
  EVENT ALTUSER
 SUMMARY USER
END
```

END Subcommand

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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

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

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

© Copyright IBM Corp. 1993, 2024

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

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

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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

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

This information may contain examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

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

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on IBM Copyright and trademark information (https://www.ibm.com/legal/copytrade).

Terms and Conditions for Product Documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal Use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or

reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see:

- The section entitled **IBM Websites** at IBM Privacy Statement (https://www.ibm.com/privacy)
- Cookies and Similar Technologies (https://www.ibm.com/privacy#Cookies_and_Similar_Technologies)

Bibliography

This topic lists the publications in the z/VM library. For abstracts of the z/VM publications, see *z/VM: General Information*.

Where to Get z/VM Information

The current z/VM product documentation is available in IBM Documentation - z/VM (https://www.ibm.com/docs/en/zvm).

z/VM Base Library

Overview

- *z/VM: License Information*, GI13-4377
- *z/VM: General Information*, GC24-6286

Installation, Migration, and Service

- *z/VM: Installation Guide*, GC24-6292
- *z/VM: Migration Guide*, GC24-6294
- *z/VM: Service Guide*, GC24-6325
- *z/VM: VMSES/E Introduction and Reference*, GC24-6336

Planning and Administration

- *z/VM: CMS File Pool Planning, Administration, and Operation*, SC24-6261
- *z/VM: CMS Planning and Administration*, SC24-6264
- *z/VM: Connectivity*, SC24-6267
- *z/VM: CP Planning and Administration*, SC24-6271
- *z/VM: Getting Started with Linux on IBM Z*, SC24-6287
- *z/VM: Group Control System*, SC24-6289
- *z/VM: I/O Configuration*, SC24-6291
- *z/VM: Running Guest Operating Systems*, SC24-6321
- *z/VM: Saved Segments Planning and Administration*, SC24-6322
- *z/VM: Secure Configuration Guide*, SC24-6323

Customization and Tuning

- *z/VM: CP Exit Customization*, SC24-6269
- *z/VM: Performance*, SC24-6301

Operation and Use

- *z/VM: CMS Commands and Utilities Reference*, SC24-6260
- *z/VM: CMS Primer*, SC24-6265
- *z/VM: CMS User's Guide*, SC24-6266
- *z/VM: CP Commands and Utilities Reference*, SC24-6268

© Copyright IBM Corp. 1993, 2024

- *z/VM: System Operation*, SC24-6326
- *z/VM: Virtual Machine Operation*, SC24-6334
- *z/VM: XEDIT Commands and Macros Reference*, SC24-6337
- *z/VM: XEDIT User's Guide*, SC24-6338

Application Programming

- *z/VM: CMS Application Development Guide*, SC24-6256
- *z/VM: CMS Application Development Guide for Assembler*, SC24-6257
- *z/VM: CMS Application Multitasking*, SC24-6258
- *z/VM: CMS Callable Services Reference*, SC24-6259
- *z/VM: CMS Macros and Functions Reference*, SC24-6262
- *z/VM: CMS Pipelines User's Guide and Reference*, SC24-6252
- *z/VM: CP Programming Services*, SC24-6272
- *z/VM: CPI Communications User's Guide*, SC24-6273
- *z/VM: ESA/XC Principles of Operation*, SC24-6285
- *z/VM: Language Environment User's Guide*, SC24-6293
- *z/VM: OpenExtensions Advanced Application Programming Tools*, SC24-6295
- *z/VM: OpenExtensions Callable Services Reference*, SC24-6296
- *z/VM: OpenExtensions Commands Reference*, SC24-6297
- *z/VM: OpenExtensions POSIX Conformance Document*, GC24-6298
- *z/VM: OpenExtensions User's Guide*, SC24-6299
- *z/VM: Program Management Binder for CMS*, SC24-6304
- *z/VM: Reusable Server Kernel Programmer's Guide and Reference*, SC24-6313
- *z/VM: REXX/VM Reference*, SC24-6314
- *z/VM: REXX/VM User's Guide*, SC24-6315
- *z/VM: Systems Management Application Programming*, SC24-6327
- *z/VM: z/Architecture Extended Configuration (z/XC) Principles of Operation*, SC27-4940

Diagnosis

- *z/VM: CMS and REXX/VM Messages and Codes*, GC24-6255
- *z/VM: CP Messages and Codes*, GC24-6270
- *z/VM: Diagnosis Guide*, GC24-6280
- *z/VM: Dump Viewing Facility*, GC24-6284
- *z/VM: Other Components Messages and Codes*, GC24-6300
- *z/VM: VM Dump Tool*, GC24-6335

z/VM Facilities and Features

Data Facility Storage Management Subsystem for z/VM

- *z/VM: DFSMS/VM Customization*, SC24-6274
- *z/VM: DFSMS/VM Diagnosis Guide*, GC24-6275
- *z/VM: DFSMS/VM Messages and Codes*, GC24-6276
- *z/VM: DFSMS/VM Planning Guide*, SC24-6277

- *z/VM: DFSMS/VM Removable Media Services*, SC24-6278
- *z/VM: DFSMS/VM Storage Administration*, SC24-6279

Directory Maintenance Facility for z/VM

- *z/VM: Directory Maintenance Facility Commands Reference*, SC24-6281
- *z/VM: Directory Maintenance Facility Messages*, GC24-6282
- *z/VM: Directory Maintenance Facility Tailoring and Administration Guide*, SC24-6283

Open Systems Adapter

- Open Systems Adapter/Support Facility on the Hardware Management Console (https://www.ibm.com/docs/en/SSLTBW_2.3.0/pdf/SC14-7580-02.pdf), SC14-7580
- Open Systems Adapter-Express ICC 3215 Support (https://www.ibm.com/docs/en/zos/2.3.0?topic=osa-icc-3215-support), SA23-2247
- Open Systems Adapter Integrated Console Controller User's Guide (https://www.ibm.com/docs/en/SSLTBW_2.3.0/pdf/SC27-9003-02.pdf), SC27-9003
- Open Systems Adapter-Express Customer's Guide and Reference (https://www.ibm.com/docs/en/SSLTBW_2.3.0/pdf/ioa2z1f0.pdf), SA22-7935

Performance Toolkit for z/VM

- *z/VM: Performance Toolkit Guide*, SC24-6302
- *z/VM: Performance Toolkit Reference*, SC24-6303

The following publications contain sections that provide information about z/VM Performance Data Pump, which is licensed with Performance Toolkit for z/VM.

- *z/VM: Performance*, SC24-6301. See z/VM Performance Data Pump.
- *z/VM: Other Components Messages and Codes*, GC24-6300. See Data Pump Messages.

RACF Security Server for z/VM

- *z/VM: RACF Security Server Auditor's Guide*, SC24-6305
- *z/VM: RACF Security Server Command Language Reference*, SC24-6306
- *z/VM: RACF Security Server Diagnosis Guide*, GC24-6307
- *z/VM: RACF Security Server General User's Guide*, SC24-6308
- *z/VM: RACF Security Server Macros and Interfaces*, SC24-6309
- *z/VM: RACF Security Server Messages and Codes*, GC24-6310
- *z/VM: RACF Security Server Security Administrator's Guide*, SC24-6311
- *z/VM: RACF Security Server System Programmer's Guide*, SC24-6312
- *z/VM: Security Server RACROUTE Macro Reference*, SC24-6324

Remote Spooling Communications Subsystem Networking for z/VM

- *z/VM: RSCS Networking Diagnosis*, GC24-6316
- *z/VM: RSCS Networking Exit Customization*, SC24-6317
- *z/VM: RSCS Networking Messages and Codes*, GC24-6318
- *z/VM: RSCS Networking Operation and Use*, SC24-6319
- *z/VM: RSCS Networking Planning and Configuration*, SC24-6320

TCP/IP for z/VM

- *z/VM: TCP/IP Diagnosis Guide*, GC24-6328
- *z/VM: TCP/IP LDAP Administration Guide*, SC24-6329
- *z/VM: TCP/IP Messages and Codes*, GC24-6330
- *z/VM: TCP/IP Planning and Customization*, SC24-6331
- *z/VM: TCP/IP Programmer's Reference*, SC24-6332
- *z/VM: TCP/IP User's Guide*, SC24-6333

Prerequisite Products

Device Support Facilities

- Device Support Facilities (ICKDSF): User's Guide and Reference (https://www.ibm.com/docs/en/SSLTBW_2.5.0/pdf/ickug00_v2r5.pdf), GC35-0033

Related Products

XL C++ for z/VM

- *XL C/C++ for z/VM: Runtime Library Reference*, SC09-7624
- *XL C/C++ for z/VM: User's Guide*, SC09-7625

z/OS

IBM Documentation - z/OS (https://www.ibm.com/docs/en/zos)

Index

Special Characters

79, 81, 84, 87, 90

A

access attempts
    auditing access attempts to resources with security labels 15
    auditing by class 14, 40
    specifying logging for detected 12
access control 1
accountability 1
activating a system z/VM event profile 22
activating an individual z/VM event profile 25
activities of group-OPERATIONS users 11
activities of OPERATIONS users 11
adding z/VM events to a system z/VM event profile 21
adding z/VM events to an individual z/VM event profile 24
administration control 9
ALL option
    for auditing CP commands 35
ALLOWED operand 105
ALTER universal access authority
    in the selected data set report 90
ALTUSER command
    logging RACF-related activities of a user 112
    UAUDIT/NOUAUDIT operand 18
    using when auditing 18
ASCEND operand 106
ATLDIR command
    GLOBALAUDIT operand 18
ATLFILE command
    GLOBALAUDIT operand 18
attribute
    AUDITOR attribute 1, 86, 88
    group AUDITOR 1
    group-OPERATIONS
        logging activities for 13
    group-SPECIAL
        bypassing the logging of activities for 12
        logging activities for 12
    OPERATIONS
        logging activities for 13
    OPERATIONS attribute 86, 88
    REVOKE attribute 86, 88
    SPECIAL
        bypassing the logging of activities for 12
        logging activities for 12
    SPECIAL attribute 1, 86, 88
ATTRIBUTE TYPE column heading
    in the selected user attribute report 86, 88
audit controls
    general audit controls 11
AUDIT operand
    SETROPTS command 12
audit records 46
audit tools 1
auditing
    access attempts by class 14, 40
    access attempts to resources with security labels 15
    OpenExtensions VM events 39, 40
    selected z/VM events 20
auditing access attempts
    example 17
auditing based on SECLABEL profiles
    example 17
auditing CP commands
    using the ALL option 35
    using the TO option 35
auditing events 20
auditing file printing
    by CP 39
auditing mandatory access checks
    by SECLABEL for profiles 36
    by SECLABEL for resources 36
auditing profile changes
    example 17
auditing restricted segments (RSTDSEG) 36
auditing with the SECLABEL option
    the CHANGE command 35
auditor
    asking security questions 5
    audit tools provided 1
    auditor-controlled logging 3
    concept of accountability 1
    controlling auditing 2
    group-wide auditor responsibilities 1
    listing specific audit controls 19
    logging specific events 2
    obtaining reports 91
    overriding owner-controlled logging
        specifying audit controls 3
        using the RACROUTE REQUEST=AUTH exit routine 3
    responsibilities 1
    setting audit controls 11
    specific audit controls 17
    specifying general audit controls
        AUDIT/NOAUDIT 11
        CMDVIOL/NOCMDVIOL 11
        LIST 11
        LOGOPTIONS 11
        OPERAUDIT/NOOPERAUDIT 11
        REFRESH GENERIC 11
        SAUDIT/NOSAUDIT 11
        SECLABELAUDIT/NOSECLABELAUDIT 11
        SECLEVELAUDIT/NOSECLEVELAUDIT 11
    system-wide auditor responsibilities 1
    use of DSMON 75
    use of the warning indicator 110
    using RACF report writer 5, 91
    verifying owner-controlled logging 2
AUDITOR attribute
    auditing for z/VM events

AUDITOR attribute *(continued)*
auditing for z/VM events *(continued)*
using the SETEVENT command 20
auditing RACF system 1
AUDITOR suboperand of AUTHORITY operand 100
AUDITOR suboperand of REASON operand 100
controlling auditing 11
list of users with 86, 88
needed to run DSMON 75
specifying audit controls 18
specifying general audit controls
AUDIT/NOAUDIT 11
CMDVIOL/NOCMDVIOL 11
LIST 11
LOGOPTIONS 11
REFRESH GENERIC 11
SAUDIT/NOSAUDIT 11
SECLABELAUDIT/NOSECLABELAUDIT 11
AUTHORITY operand
AUDITOR suboperand 100
BYPASSED suboperand 100
EXIT suboperand 100
FAILSOFT suboperand 100
NORMAL suboperand 100
OPERATIONS suboperand 100
SPECIAL suboperand 100
authorization requests
auditing not done 14, 40

B

basic z/OS system 6
basic z/VM system 6
BY(name2) operand 107
bypassing
logging of activities for SPECIAL attribute 12
logging of RACF command violations 13

C

CHANGE command
auditing with the SECLABEL option 35
CLASS operand 104
class-descriptor table report
description 80, 82
use of 80, 82
command and subcommand processing
described 92
END subcommand 92
EVENT subcommand 92
LIST subcommand of RACFRW command 92
RACF report writer 92
RACRPORT EXEC 92
SELECT subcommand 92
SUMMARY subcommand 92
command violations
auditing 17
command-summary report 111
commands
RACF
entering a RACF command session on z/VM 2
using the RAC command processor on z/VM 2
communication between z/VM users
communication between z/VM users *(continued)*
auditing z/VM events 20
COMPATMODE suboperand
COMPATMODE suboperand of REASON operand 100
CONTROL universal access authority
in the selected data set report 90
control user access 1
controlling auditing 2
controlling logging
by auditor 3
by owner 2
CP commands
auditing 20
CPU MODEL column heading
in the system report 78
CPU-ID column heading
in the system report 78
creating a system z/VM event profile 21
creating an individual z/VM event profile 24

D

DATA operand
RACFRW command 96
DATA SET NAME column heading
in the selected data set report 89
DATASET class
auditing for 12
DATE operand 99
DEFINE MDISK, auditing for 36
deleting an individual z/VM event profile 26
DESCEND operand 106
DIAGNOSE functions
auditing 20
DSMON (data security monitor)
class-descriptor table report 80, 82
control statements
LINECOUNT 76
USEROPT 77
control statements for DSMON functions 76
description 75
functions for generating reports 77
generated by DSMON
class-descriptor table report 80, 82
global access-checking table report 84, 85
group tree report 79
global access checking report 84, 85
group tree report 79
how to run 75
list of reports produced 78
RACDSMON 75
RACF exits report 83, 84
selected data-sets report 89, 90
selected user-attribute report 86, 88
selected user-attribute summary report 88
system report 78

E

END subcommand of RACFRW command
description 108
EVENT subcommand of RACFRW command
ALLOWED operand 105

EVENT subcommand of RACFRW command *(continued)*
CLASS operand 104
dependency of SELECT subcommand 101
described 101
EVENT subcommand operand combination table 104
event-name operand 102
event-name operand values listed 103
EVQUAL operand 104
INTENT operand 105
issued with SELECT subcommand 98
LEVEL operand 105
monitoring access violations 111, 113, 114
NAME operand 104
NEWNAME operand 105
password violation levels 109
syntax 102
event-name operand 102
events, auditing 20
EVQUAL operand 104
EXIT MODULE NAME column heading
in the RACF exits report 84

F

failsoft processing
logging 2
FORMAT operand
RACFRW command 96
FUNCTION control statement
control statements
FUNCTION 77
DSMON (data security monitor) 77
functions
that DSMON uses to generate reports 77

G

general audit controls
how to use 11
general resource class
auditing for 12
general resource controls 18
GENSUM operand
RACFRW command 97
global access checking
auditing not done 14, 15
global access-checking table report
description 84, 85
use of 84, 85
group AUDITOR attribute
responsibility limits defined 1
GROUP operand 100
group tree report
description 79
use of 79
group-AUDITOR attribute
list of users with 86, 88
restriction for controlling auditing 11
specifying audit controls 18
specifying general audit controls
LIST 11
REFRESH GENERIC 11
group-OPERATIONS attribute
group-OPERATIONS attribute *(continued)*
list of users with 86, 88
logging activities for 13
monitoring group-OPERATIONS users 112
group-REVOKE attribute
list of users with 86, 88
group-SPECIAL attribute
bypassing the logging of activities for 12
list of users with 86, 88
logging activities for 12
logging activities of 11
monitoring group-SPECIAL users 112

I

ICHRSMFE exit routine 91
ICHRSMFI module
SORTEQU field 106
individual z/VM event profile
activating an individual z/VM event profile 25
adding z/VM events to an individual z/VM event profile 24
creating an individual z/VM event profile 24
deleting an individual z/VM event profile 26
description 23
stopping the auditing of a specific z/VM Event in an individual z/VM event profile 25
suspending an individual z/VM event profile 25
using individual z/VM event profiles to control auditing 24
installation access control 1
installation accountability 1
installation exit ICHRSMFE 91
installation-replaceable module ICHRSMFI 91
INTENT operand 105
Interactive System Productivity Facility (ISPF) program 2
IRRADU00 utility
using on z/VM (RACFADU) 49
IRRDBU00 utility
auditor's use of 4
SQL/DS table names 54
SQL/DS utility statements required to delete the group records 54
IRRUT100 utility
auditor's use of 4
ISPF panels
compared to RACF commands 3
ISPF program 2

J

JOB operand 100

L

LAST SYSTEM GENERATION column heading
in the system report 79
LAST SYSTEM IPL column heading
in the system report 79
LDIRECT command
using when auditing 19
LEVEL operand 105
LFILE command

LFILE command *(continued)*
using when auditing 19
LINECNT operand
RACFRW command 97
LINECOUNT control statement
DSMON (data security monitor) 76
LINK event name
audit records 38
LIST subcommand of RACFRW command
ASCEND operand 106
DESCEND operand 106
description 105
NEWPAGE operand 106
restrictions 105
SORT operand 106
syntax 105
TITLE operand 106
LISTDSD command 2, 19
LISTGRP command 2, 19
listing specific audit controls
described 19
LDIRECT command 19
LFILE command 19
LISTDSD command 19
LISTGRP command 19
LISTUSER command 19
RLIST command 19
LISTUSER command 2, 19
logging
access attempts based on security level 13
access levels 2
accesses to resources at specific audit levels 3
accesses to resources within a certain SECLABEL 3
accesses to specific data sets 3
accesses to specific general resources 3
activities for OPERATIONS attribute 13
activities for SPECIAL attribute 12
activities of group-OPERATIONS users 11
activities of group-SPECIAL users 11
activities of OPERATIONS users 11
activities of SPECIAL users 11
all RACF-related activities for users 17
attempts to access DASD data sets 17
attempts to access general resources 17
attempts to access RACF-protected resources 18
attempts to access resources protected by a SECLABEL 17
auditor-controlled logging 3
bypassing for users with SPECIAL attribute 12
changes to any RACF profile 3
command violations 11
deletions to profiles 18
events RACF always logs 2
events RACF never logs 2
failsoft processing 2
general audit controls 11
general resource information 18
obtaining printed reports 5
owner-controlled logging 2
profile changes 11
RACF command violations 3
RACF commands issued 18
RACF commands issued by group-SPECIAL user 3
RACF commands issued by SPECIAL user 3
logging *(continued)*
RACF data in SMF records 5
RACF-related activities 112
RACF-related activities of specific users 3
RACROUTE REQUEST=AUTH requests 3
RACROUTE REQUEST=VERIFY requests 2
selected z/VM events 20
setting audit controls 11
specific events 2
system-wide for RACF classes 12
system-wide RACF command violations 13
types of accesses 2
use of RVARY command 2
use of SETROPTS command 2
user additions to profiles 18
user changes to profiles 18
LOGON BY
auditing 45, 46
determining relationships 46
surrogate user 45, 46
LOGOPTIONS operand
SETROPTS command 14, 40
LOGOPTIONS suboperand
LOGOPTIONS suboperand of REASON operand 100

M

management control 10
mandatory access control (MAC)
see “auditing mandatory access checks” 36
MDISK event name
audit records 38
messages
RACF exits report 84
selected data sets report 90
system report 79
minidisk
for recording SMF records 41
miscellaneous security concerns 6
modifying resource profile 3
MODULE LENGTH column heading
in the RACF exits report 84
monitoring access attempts
by security label 113
by security level 113
in warning mode 110
monitoring access violations
UACC, monitoring use of 111
with RACF report writer 111
with RACFRW command 113, 114
monitoring OPERATIONS users
with RACF report writer 112
with RACFRW command 113
monitoring password violation levels
LOGON process 109
password violation occurrences 109
password violation stabilization 109
monitoring SPECIAL users
with RACF report writer 112
with RACFRW command 112
monitoring specific users
with RACF report writer 112
with RACFRW command, by specified user 112
monitoring use of RACF commands

monitoring use of RACF commands *(continued)*
with RACF report writer 111
with RACFRW command, by specified user 112
with RACFRW command, by users 111
monitoring while deferring access decisions
with RACF report writer 111

N

NAME operand
EVENT subcommand of RACFRW command 104
name1 operand
SUMMARY subcommand of RACFRW command 107
NEWNAME operand 105
NEWPAGE operand
LIST subcommand of RACFRW command 106
SUMMARY subcommand of RACFRW command 108
NOCMDVIOL operand
SETROPTS command 13
NOFORMAT operand
RACFRW command 97
NOGENSUM operand
RACFRW command 97
NONE universal access authority
in the selected data set report 90
NOOWNER operand 100
NOSAUDIT operand
SETROPTS command 12
NOUSER operand
SELECT subcommand of RACFRW command 99

O

obtaining printed reports from DSMON 75
obtaining printed reports from the report writer 5
OpenExtensions VM
auditable events 39
auditing considerations 39
auditing options 40
commands 40
controlling auditing
classes 39
OPERATING SYSTEM/LEVEL column heading
in the system report 78
OPERATIONS attribute
list of users with 86, 88
logging activities for 13
monitoring OPERATIONS users 112
OPERATIONS suboperand of AUTHORITY operand 100
OPERATIONS user
auditing 16
OPERAUDIT operand
SETROPTS command 13
overriding user specification 18
OWNER operand 100
owner-controlled logging
done by resource owner 2
listing specific audit controls 19
overridden by auditor 2
overriding user specification 18

P

panels
using 2
password violation levels
calculating percentages 109
example 109
monitoring 109
printed reports
from DSMON 75
from the RACF report writer 5
PROCESS operand
SELECT subcommand of RACFRW command 100
PROCESS records 93
protection plan 7

R

RACDSMON EXEC 75
RACF
access control 1
accountability 1
attributes 1
audit tools provided
audit control functions 2
DSMON 2
logging routines 2
RACF report writer 2
RACF SMF data unload utility 2
commands
LDIRECT command 2
LFILE command 2
LISTDSD command 2
LISTGRP command 2
LISTUSER command 2
RLIST command 2
SEARCH command 2
SETROPTS command 11
SRDIR command 2
SRFILE command 2
controlling auditing 2
defined 1
panels 2
user responsibilities
auditor's role (user with AUDITOR attribute) 1
security administrator's role (user with SPECIAL attribute) 1
RACF auditor 1
RACF command
entering a RACF command session on z/VM 2
using the RAC command processor on z/VM 2
RACF commands
ALTUSER command 18, 112
bypassing logging of violations 13
compared to ISPF panels 3
LDIRECT command 2, 19
LFILE command 2, 19
LISTDSD command 2, 19
LISTGRP command 2, 19
LISTUSER command 2, 19
logging activity for specified classes 12
RALTER command 19
RLIST command 2, 19
RVARY command 2

RACF commands *(continued)*
SEARCH command 2
SETROPTS command
monitoring access to resources with a security label 114
monitoring access to resources with a security level 113
monitoring SPECIAL users 112
SRDIR command 2
SRFILE command 2
RACF exits report
description 83, 84
messages 84
use of 83, 84
RACF implementation 7
RACF implementation/integrity 6
RACF INDICATED field
in the selected data set report 89
RACF PROTECTED field
in the selected data set report 89
RACF report writer
command description 94
compared to RACF commands 5
default values 93
examples 114
installation exit ICHRSMFE 91
installation-replaceable module ICHRSMFI 91
merging RACF for z/VM SMF records with RACF for z/OS SMF records 43
monitoring
deferring access decisions 111
monitoring access attempts by security label 113
monitoring access attempts by security level 113
monitoring access attempts in WARNING mode 110
monitoring of
access violations 111
RACF commands 111
monitoring of specific users 112
monitoring OPERATIONS users 112
monitoring password violation levels 109
monitoring SPECIAL users 112
obtaining reports 91
overview 92
record selection criteria 98
report generation 93
report types
access to RACF-protected resource 91
descriptions of group activity 91
descriptions of user activity 91
summaries of resource use 91
summaries of system use 91
return codes from 95
sample RACFRW CONTROL files 130
SMF record types 93
SMF records 5
subcommand description 94
terminal monitor program 94
TMP 94
use of SMF records 93
use of work data set 93
using 5
warning mode example 110
RACF Report Writer 91
RACF SMF data unload
RACF SMF data unload *(continued)*
description 49
operational considerations 49
RACF SMF data unload utility
creating a SQL/DS DBSPACE 53
creating the SQL/DS tables 53
using 5, 49, 60
using with SQL/DS 52, 53
RACFADU
panel invocation 50
setup 49
used to execute IRRADU00 on z/VM 49
RACFADU EXEC
command invocation
return codes 52
input panel 50
RACFADU utility
auditor's use of 5
deleting data from the SQL/DS database 54
loading the SQL/DS tables 54
reorganizing the indexes in the SQL/DS database 54
RACFRW command
command syntax 94
DATA operand 96
default maximum record length 93
description 96
END subcommand 108
EVENT subcommand 101
FORMAT operand 96
GENSUM operand 94, 97
LINECNT operand 97
LIST subcommand of RACFRW command 105
monitoring of
access violations 111, 113, 114
OPERATIONS users 113
RACF commands 111
RACF commands issued by user 112
SPECIAL users 112
specific users 112
NOFORMAT operand 97
NOGENSUM operand 97
sample reports 116
SELECT subcommand 97
subcommand description 94
SUMMARY subcommand 107
syntax 96
TITLE operand 96
using RACF report writer 5
warning mode example 110
RACFRW CONTROL files
samples 130
RACFSMF user ID 43
RACROUTE REQUEST=AUTH requests 3
RACROUTE REQUEST=DEFINE requests
logging activity for specified classes 12
RACROUTE REQUEST=VERIFY requests 2
RALTER command
GLOBALAUDIT operand 18
overriding user specification 18
using when auditing 19
RDEVCTRL event name
audit records 38
READ universal access authority
in the selected data set report 90

read-only auditor
group-wide auditor responsibilities 1
system-wide auditor responsibilities 1
REASON operand
AUDITOR suboperand 100
CLASS suboperand 100
CMDVIOL suboperand 100
COMMAND suboperand 100
RACINIT suboperand 100
RESOURCE suboperand 100
SPECIAL suboperand 100
USER suboperand 100
record selection
RACF report writer 93
records
PROCESS records 93
SMF records 93
STATUS records 93
REFRESH GENERIC operands
SETROPTS command 15
refreshing in-storage generic profiles
example 17
report writer
sample output for shared user IDs 129
reports
access to RACF-protected resource 91
descriptions of group activity 91
descriptions of user activity 91
general summary 120
generated by DSMON
RACF exits report 83, 84
selected data-sets report 89, 90
selected user-attribute report 86, 88
selected user-attribute summary report 88
system report 78
list of summaries from the report writer 107
listing of status 121
produced by DSMON 78
RACFRW sample reports 116
standard header page for report writer 120
summaries of resource use 91
summaries of system use 91
summary
group activity 123
group activity by resource 126
owner activity 125
owner activity by resource 118, 129
RACF command activity 124
RACF command activity by group 129
RACF command activity by resource 129
RACF command activity by user 128
resource activity 124
resource activity by group 127
resource activity by resource 126
resource activity by security event 127
security event activity 125
security event activity by resource 128
user activity 123
user activity by resource 125
resource owners
controlling logging 2
responsibilities of auditors 1
restricted segments (RSTDSEG)
restricted segments (RSTDSEG) *(continued)*
auditing 36
return codes
from RACF report writer 95
REVOKE attribute
list of users with 86, 88
RLIST command
using when auditing 19
ROAUDIT attribute 1
RSTDSEG (restricted segments)
auditing 36
RVARY command 2

S

sample
report writer output for shared user IDs 129
sample reports
from the report writer 116
SAUDIT operand
SETROPTS command 12
SEARCH command
listing profiles that have the warning indicator 110
SECAUDIT suboperand
SECAUDIT suboperand of REASON operand 100
SECLABEL auditing
related system overhead 15
using the SECLABELAUDIT function 15
SECLABEL option
using to audit the CHANGE command 35
SECLABELAUDIT function
for auditing security labels 15
related system overhead 15
SECLABELAUDIT operand
SETROPTS command 15
SECLABELAUDIT suboperand
SECLABELAUDIT suboperand of REASON operand 100
SECLEVELAUDIT operand
SETROPTS command 13
security administrator
monitoring SPECIAL users 112
SPECIAL attribute 1
use of RACF commands 111
security labels
auditing access attempts to resources with security labels 15
security level
auditing access attempts 17
logging access attempts based on 13
SELECT subcommand of RACFRW command
AUTHORITY operand 100
DATE operand 99
dependency of EVENT subcommand 101
GROUP operand 100
issued with EVENT subcommand 98
JOB operand 100
monitoring access violations 111, 113, 114
monitoring OPERATIONS users 113
monitoring SPECIAL users 112
monitoring specific users 112
monitoring use of RACF commands by user 112
NOOWNER operand 100
NOUSER operand 99
OWNER operand 100

SELECT subcommand of RACFRW command *(continued)*
password violation levels 109
PROCESS operand 100
RACFRW command 97
REASON operand 100
restrictions 98
STATUS operand 100
STEP operand 100
SUCCESSES operand 99
syntax 99
SYSID operand 100
TERMINAL operand 101
USER operand 99
VIOLATIONS operand 99
warning mode example 110
WARNINGS operand 99
selected data-sets report
description 89, 90
messages 90
use of 89, 90
selected user-attribute report
description 86, 88
selected user-attribute summary report
description 88
SELECTION CRITERION column heading
in the selected data set report 89
SETEVENT command
auditing z/VM events 20
SETROPTS command
AUDIT/NOAUDIT operands 11
CMDVIOL/NOCMDVIOL operands 11
LIST operand
LOGOPTIONS 11
SECLABELAUDIT/NOSECLABELAUDIT 11
logging use of 2
monitoring access to resources with a security label 114
monitoring access to resources with a security level 113
monitoring group-SPECIAL users 112
monitoring SPECIAL users 112
operands for auditing 11
REFRESH GENERIC operands 11, 15
SAUDIT operand 112
SAUDIT/NOSAUDIT operands 11
SECLABELAUDIT 114
SECLEVELAUDIT operand 113
setting audit controls 11
shared user ID
auditing on z/VM 45, 46
SURROGAT class 46
verifying 46
SMF CONTROL file
setting up 41
SMF data unload utility
merging RACF for z/VM SMF records with RACF for z/OS SMF records 43
SMF data unload, output to XML 57
SMF on z/VM
editing the SMF control file 41
minidisks 42
SMF records
listing contents of 91
PROCESS records 93
RACF report writer 91
specifying the format of 42
SMF records *(continued)*
STATUS records 93
types
type 20 93
type 30 93
type 80 93
type 81 93
type 83 93
used by RACF report writer 93
SMFPROF EXEC 43
SORT operand 106
SPECIAL attribute
bypassing the logging of activities for 12
list of users with 86, 88
logging activities for 12
monitoring SPECIAL users 112
SPECIAL suboperand of AUTHORITY operand 100
SPECIAL suboperand of REASON operand 100
special considerations
for auditors 47
SPECIAL user
auditing 16
specific audit controls
all RACF-related activities for users 17
attempts to access DASD data sets 17
attempts to access general resources 17
attempts to access resources protected by a SECLABEL 17
specific user controls
general resource controls 18
listing specific audit controls 19
use of ALTUSER command 18
specifying audit controls 3
SQL/DS
creating a DBSPACE 53
creating tables 53
loading the SQL/DS tables for RACF SMF data unload formatted records 54
SQL/DS utility statements required to delete the group records 54
table names provided in SAMPLE files 54
using with the RACF SMF data unload utility 53
SQL/DS database
deleting the IRRDBU00 data from the SQL/DS database 54
SQL/DS Database
reorganizing the indexes in the SQL/DS database 54
SRDIR command 2
SRFILE command 2
standard header page for report writer 120
START auditing
command 38
of a real printer 38
STATUS operand 100
STATUS records 93
STEP operand 100
stopping auditing
specific z/VM event
in a system z/VM event profile 22
stopping the auditing of a specific z/VM Event in an individual z/VM event profile 25
SUCCESSES operand
SUMMARY subcommand of RACFRW command 108
summary reports from the report writer 107

SUMMARY subcommand of RACFRW command
  BY(name2) operand 107
  description 107
  monitoring use of RACF commands 111
  name1 operand 107
  NEWPAGE operand 108
  SUCCESSES operand 108
  syntax 107
  TITLE operand 108
  used with EVENT subcommand 107
  used with SELECT subcommand 107
  VIOLATIONS operand 108
  WARNINGS operand 108
SURROGAT class 46
surrogate user
  auditing 45
  identifying 45, 46
  SURROGAT class 46
  verifying 46
suspending an individual z/VM event profile 25
SYSID operand 100
system information 6
system report
  description 78
  messages 79
  produced when RACF is inactive 75
  sample 79
  use of 78
system z/VM event profile
  activating a system z/VM event profile 22
  adding z/VM events to a system z/VM event profile 21
  creating a system z/VM event profile 21
  description 21
  stopping auditing
    in a system z/VM event profile 22
system-wide audit controls 11
system-wide auditor responsibilities 1

T

technical security concerns 8
terminal monitor program 94
TITLE operand
  RACFRW command 96
  SUMMARY subcommand of RACFRW command 108
TMP (terminal monitor program) 94
TO option
  for auditing CP commands 35
TOTAL DEFINED USERS column heading
  in the selected attribute summary report 88
TOTAL SELECTED ATTRIBUTE USERS column heading
  in the selected attribute summary report 88
type 20 SMF record 93
type 30 SMF record 93
type 80 SMF record 93
type 81 SMF record 93
type 83 SMF record 93

U

UACC
  monitoring the use of 111
UACC field
UACC field *(continued)*
  in the selected data set report 90
UPDATE universal access authority
  in the selected data set report 90
usage of attributes 7
user attribute 1
user controls 18
user ID
  shared 45, 46
  surrogate 45, 46
USER operand 99
user-controlled logging
  done by resource owner 2
  overridden by auditor 2
user-written exit routine ICHRSMFE 91
user-written module ICHRSMFI 91
USERID column heading
  in the selected user attribute report 86, 88
USEROPT control statement
  DSMON (data security monitor) 77
using individual z/VM event profiles to control auditing 24
using LOGON BY
  audit records 46
  special considerations 47
utility messages 52

V

verify user access 1
VIOLATIONS operand 99, 108
VMXEVENT profile
  member names 26
VOLUME SERIAL column heading
  in the selected data set report 89

W

warning indicator 110
warning mode
  cautions when using 110
  defined 110
  monitoring access attempts in 110
  report example 110
  warning indicator 110
WARNING operand
  SEARCH command 110
WARNINGS operand
  SELECT subcommand of RACFRW command 99
  SUMMARY subcommand of RACFRW command 108
work data set 93

X

XML, obtaining output from SMF data unload 57

Z

z/VM events
  auditing 20
  individual z/VM event profile
    activating an individual z/VM event profile 25
    creating an individual z/VM event profile 24
    deleting an individual z/VM event profile 26

z/VM events *(continued)*
individual z/VM event profile *(continued)*
stopping the auditing of a specific z/VM event in an individual z/VM event profile 25
suspending an individual z/VM event profile 25
RACF names for 26
z/VM Events
individual z/VM event profile
adding z/VM events to an individual z/VM event profile 24
description 23
using individual z/VM event profiles to control auditing 24
system z/VM event profile
activating a system z/VM event profile 22
adding z/VM events to a system z/VM event profile 21
creating a system z/VM event profile 21
description 21
stopping auditing 22

Product Number: 5741-A09

Printed in USA

SC24-6305-74