Enhanced Auditing Using the RACF SMF Data Unload Utility

Document Number GG24-4453-00

October 1994

International Technical Support Organization
Poughkeepsie Center

Take Note!

Before using this information and the product it supports, be sure to read the general information under “Special Notices” on page xi.

First Edition (October 1994)

This edition applies to Version 2, Release 1 of Resource Access Control Facility, Program Number 5695-039 for use with the MVS/ESA

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

An ITSO Technical Bulletin Evaluation Form for reader's feedback appears facing Chapter 1. If the form has been removed, comments may be addressed to:

IBM Corporation, International Technical Support Organization
Dept. 541 Mail Station P099
522 South Road
Poughkeepsie, New York 12601-5400

Abstract

This document describes a number of RACF auditing tools that are based on the RACF SMF Data Unload Utility and on the RACF Database Unload Utility. The primary audience is RACF security auditors. This document provides the information that is necessary to compile the sample code into a service offering.

The RACF SMF Data Unload Utility enables installations to create a sequential file from the SMF security-relevant audit data. The RACF Database Unload Utility unloads the RACF database to a sequential file. Both sequential files can be used in several ways: viewed directly, used as input for installation-written programs, and manipulated with sort/merge utilities.

These sequential files can also be uploaded to a database manager to process complex inquires and create installation-tailored reports. The auditing tools that are described in this book are based on DB2 or DB2/2 as the database manager.

(68 pages)

Contents

Figures

Tables

Special Notices

This publication is intended to help Resource Access Control Facility (RACF) auditors and administrators to get a better picture of the contents in the RACF database and to verify that the installation security policy is not compromised.

The information in this publication is not intended as the specification of any programming interfaces that are provided by the Query Management Facility (QMF) and the Visualizer Query for OS/2 products. See the PUBLICATIONS section of the IBM Programming Announcement for QMF and Visualizer Query for OS/2 for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM′s product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM′s intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer′s ability to evaluate and integrate them into the customer′s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

The following terms, which are denoted by an asterisk (*) in this publication, are trademarks of the International Business Machines Corporation in the United States and/or other countries:

CICS	DATABASE 2
DB2	DB2/2
Distributed Database Connection Services/2	IBM
MVS/ESA	OpenEdition
Operating System/2	OS/2
OS/400	PS/2
QMF	RACF
SQL/DS	SystemView

Other trademarks are trademarks of their respective companies.

Preface

This document is intended to give data security auditors an overview of the various tools that are available to audit a RACF environment. It also describes an application that is used to assist in both RACF security administration and RACF auditing. The application is based on the *RACF Database Unload Utility*, which became available in RACF Version 1 Release 9, and the *RACF SMF Data Unload Utility*, available with RACF Version 2 Release 1.

The document is primarily intended for RACF auditors, but RACF security administrators might also find the information useful.

How This Document is Organized

The document is organized as follows:

- Chapter 1, “Introduction”

  This chapter provides an overview of the tasks that an auditor needs to perform and the tools that are available to assist him in these tasks.

- Chapter 2, “Auditing Tools”

  This chapter discusses the various ways in which an auditor can find necessary auditing information. This chapter also provides some sample reports that are produced by various tools.

- Chapter 3, “The Auditing Application”

  This chapter provides an overview of an auditing application that uses ISPF, QMF and DB2 databases to produce audit reports. Software prerequisites and installation instructions are also included.

- Chapter 4, “Using the Auditing Application and Sample Reports”

  This chapter provides an overview on how to implement and use the auditing application that is described in the book.

- Chapter 5, “The Workstation Auditing Application”

  This chapter provides an alternative to auditing on the host environment. This alternative is based on IBM DATABASE 2 (DB2) and IBM DATABASE 2 OS/2 (DB2/2) on a workstation.

- Chapter 6, “The Enhanced Reporting Application”

  This chapter describes the various reports that are obtained with the enhanced reporting application. The enhanced reporting application is based on the RACF Database Unload Utility.

- Appendix A, “Sample CLIST for Starting the Report Application”

  This appendix provides a CLIST that is used to start the audit application.

Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this document.

Resource Access Control Facility (RACF)

- *RACF Auditor's Guide*, SC23-3727
- *RACF Macros and Interfaces*, SC23-3732
- *RACF Command Language Reference*, SC23-3731

Query Management Facility (QMF)

- *QMF General Information*, GC26-4713
- *QMF Learner's Guide*, SC26-4714
- *QMF Advanced User's Guide*, SC26-4715
- *QMF Reference*, SC26-4716
- *QMF Application Development Guide*, SC26-4722
- *QMF Messages and Codes*, SC26-4834
- *QMF Reference Summary*, SX26-3783

IBM DATABASE 2 (DB2) Version 2 Release 3

- *DB2 General Information*, GC26-4373
- *DB2 Administration Guide, Volume I, II, and III* , SC26-4374
- *DB2 Application Programming and SQL Guide*, SC26-4377
- *DB2 Command and Utility Reference*, SC26-4378
- *DB2 Messages and Codes*, SC26-4379
- *DB2 SQL Reference*, SC26-4380
- *DB2 Reference Summary*, SX26-3771
- *DB2 Usage of Distributed Data Management Commands*, SC26-3077

IBM DATABASE 2 OS/2 (DB2/2)

- *Information and Planning Guide*, S62G-3662
- *DB2/2 Guide*, S62G-3663
- *Installation Guide*, S62G-3664
- *Programming Guide*, S62G-3665
- *Messages and Problem Determination Guide*, S62G-3668

Communication Manager/2

- *Information and Planning Guide*, SC31-7007
- *Host Connection Reference*, SC31-6170
- *Problem Determination Guide*, SC31-6156

Distributed Database

- *SAA Introduction to Distributed Data*, GC26-4831
- *Introduction to Distributed Relational Data*, GG24-3200
- *DB2-APPC/VTAM Distributed Database Usage Guide*, GG24-3300
- *DB2 Distributed Database Application Implementation and Installation Primer*, GG24-3400
- *Distributed Relational Database Connectivity Concepts and Scenarios*, SC26-4783
- *Distributed Relational Database Application Scenarios*, GG24-3513
- *Distributed Relational Database Planning and Design Guide for DB2 Users*, GG24-3755
- *Distributed Relational Database: Using OS/2 DRDA Client Support with DB2*, GG24-3771
- *Distributed Relational Database - Cross Platform Connectivity and Application*, GG24-4311
- *Distributed Relational Database Architecture Reference*, SC26-4651
- *DRDA: Application Programming Guide*, SC26-4773
- *DDCS User's Guide*, SC09-1923
- *DDCS/2 Guide V2 with DB2/2*, S62G-3792
- *DRDA: Connectivity Guide* , SC26-4783
- *DRDA: Planning for Distributed Relational Database*, SC26-4650
- *DRDA: Problem Determination Guide*, SC26-4782

Visualizer for OS/2

- *Visualizer for OS/2: Installing and Supporting*, SH45-5087
- *Visualizer Query for OS/2: Using*, SH45-5089
- *Visualizer Development for OS/2: Introduction*, SH45-5094
- *Visualizer Development for OS/2: Reference*, SH45-5095

SystemView Enterprise Performance Data Manager/MVS (EPDM)

- *EPDM General Information*, GH19-6815
- *EPDM Administration Guide*, SH19-6816

VTAM

- *VTAM Network Implementation Guide*, SC31-6434
- *VTAM Programming for LU 6.2*, SC31-6437
- *VTAM Resource Definition Reference*, SC31-6438

REXX Publications

- *TSO/E Version 2 REXX/MVS User's Guide*, SC28-1882
- *TSO/E Version 2 REXX/MVS Reference*, SC28-1883

International Technical Support Organization Publications

- *Expanding the Capabilities of the RACF SEARCH Command*, GG66-3217

A complete list of International Technical Support Organization publications, with a brief description of each, may be found in:

Bibliography of International Technical Support Organization Technical Bulletins, GG24-3070.

To get listings of ITSO technical publications (known as “redbooks”) online, VNET users may type:

```
TOOLS SENDTO WTSCPOK TOOLS REDBOOKS GET REDBOOKS CATALOG
```

How to Order ITSO Technical Publications

IBM employees in the USA may order ITSO books and CD-ROMs using PUBORDER. Customers in the USA may order by calling 1-800-879-2755 or by faxing 1-800-284-4721. Visa and Master Cards are accepted. Outside the USA, customers should contact their local IBM office.

Customers may order hardcopy ITSO books individually or in customized sets, called GBOFs, which relate to specific functions of interest. IBM employees and customers may also order ITSO books in online format on CD-ROM collections, which contain books on a variety of products.

Acknowledgments

This publication is the result of a residency conducted at the International Technical Support Organization, Poughkeepsie Center.

The advisor for this project was:

Cees Kingma
International Technical Support Organization, Poughkeepsie Center

The authors of this document are:

Hilding Landen	IBM Sweden
Asko Raivio	IBM Finland
Ricardo Alvarez	IBM Argentina
Rainer Bauer	IBM Germany

Thanks to the following people for the invaluable advice and guidance provided in the production of this document:

Walt Farrell	RACF Design and MVS Systems Security
Mark Nelson	RACF Design

Chapter 1. Introduction

The task of an auditor basically consists of verifying that the principles set forth in an installation's security policy are not compromised. In an installation which uses the Resource Access Control Facility (RACF*) program product as its access control program, there are two main tasks to perform:

- Verifying that the RACF profiles have the proper contents (universal access, access lists and logging options in particular)
- Use the security logs to follow up on detected violations and to detect abnormal behavior by authorized users

The audit information can be quite extensive and is found in the RACF database, the RACF security log and in the logs produced by applications that use RACF services. The problem facing an auditor is mostly that of being able to reduce the amount of information to something that can be easily analyzed, and perhaps more important to be able to find the needles in some very large haystacks.

The tools available to do auditing are the normal RACF commands, the RACF Report Writer command and applications such as the Service Level Reporter (SLR) and the SystemView* Enterprise Performance Data Manager (EPDM).

With RACF Version 1 Release 9 also came the RACF Database Unload Utility which gave RACF administrators and auditors a entire new source of information. By loading the sequential output file from the utility into a relational database, such as IBM* DATABASE 2* (DB2*), they now could perform adhoc queries on the RACF database, without the risk of impairing system performance.

For the auditor to analyze RACF security logs and the SMF data in particular, the RACF Report Writer command (RACFRW) has traditionally been the main vehicle. However, auditors have long been complaining about the readability of the RACFRW output, about the inability to select events only after they exceed a given number and about the fact that the RACFRW does not limit a group auditor to the events produced within the scope of the auditor. Most installations have, therefore, written their own post processor programs to do additional processing based on the RACFRW output.

With the availability of RACF Version 2 Release 1 also came a change in the auditing functions for the system. The RACFRW command has been functionally stabilized on the RACF Version 1 Release 9.2 level, and all the new event codes can only be handled using the RACF SMF Data Unload Utility. This utility converts RACF SMF records into a sequential dataset (flat file). This dataset can be sorted and records selected based on various selection criteria. The unloaded SMF records can also be loaded into a relational database and be processed with suitable query languages.

There is a slight problem connected with the use of relational databases; users have to be taught the Structured Query Language (SQL), the Query Management Facility (QMF*) or some other query language if they want to be able to perform their own adhoc queries. The alternative is for someone to build an application with a set of predefined reports which can easily be adapted to fit the individual installation.

This takes us to the subject of this book which is an application that we started developing for our customers when the RACF Database Unload Utility became available. We have now extended this application to also handle the output from the RACF SMF Data Unload Utility. We chose the Interactive System Productivity Facility program product (ISPF) to drive this application, and to perform the actual queries we use a combination of REXX EXECs and QMF queries.

The *auditing application* that is described in this book consists of the following parts:

- A auditing application that is using the ISPF, REXX EXECs, and QMF on MVS. This application is based on the RACF SMF Data Unload Utility.
- A auditing application that is running in a OS/2* environment using DB2/2*, DDCS/2, and the Visualizer Query for OS/2. This application is also based on the RACF SMF Data Unload Utility.
- The enhanced reporting application that is using ISPF, REXX EXECs, and QMF on MVS. This application is based on the RACF Database Unload Utility.

We would have liked to written the application using only REXX and SQL, but found that it would have made the logic much more complicated and would have required a lot more programming. The QMF forms facility and EXPORT/IMPORT functions have simplified coding substantially and should make further tailoring easier.

In Chapter 2, “Auditing Tools” you will see how existing tools are used and also what restrictions are imposed on these tools. In Chapter 4, “Using the Auditing Application and Sample Reports,” we discuss in more detail how the user can use our ISPF based application to generate reports and to tailor these reports further to fit specific needs.

Since SQL is also available in DB2/2, we have looked at ways in which auditing could be done using a workstation running Operating System/2* (OS/2). Our findings are documented in Chapter 5, “The Workstation Auditing Application.”

In Chapter 6, “The Enhanced Reporting Application” on page 47, there is an explanation on how to use the original part of our application; the enhanced reporting application.

1.1 How to Order Materials Discussed in This Document

A copy of the source for these ISPF applications, the OS/2 based application and REXX procedures described in this document will be administrated by the International Technical Support Organization in Poughkeepsie. In this case “administration” means the tools package will be refreshed when required but, the code remains on a “best support” basis. The package is available on the MVSTOOLS disk under the name ASKO/2.

If you are interested in these applications, please contact your local IBM representative.

Chapter 2. Auditing Tools

There are numerous ways in which to extract information from or change information within the RACF database. This chapter provides an overview of those commands, utilities and programming languages that are either supplied with the RACF product, or are part of other IBM products, such as:

- RACF LIST commands
- RACF SEARCH command
- RACF Cross Reference Utility - IRRUT100
- REXX programs and CLISTs
- RACF Database Unload Utility
- RACF Report Writer
- RACF Data Security Monitor
- RACF SMF Data Unload Utility
- Enterprise Performance Data Manager/MVS (EPDM)

The first three facilities in this list will actually extract information from the active primary RACF database. REXX programs do not have to access the RACF database directly. There could be an intermediate step where the RACF profiles can either be extracted to a data set in a format that your program can use, or reports produced by some other means where the output is then massaged either into a more meaningful report or maybe even into RACF commands that will actually modify the RACF database.

2.1 RACF LIST Commands

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

The following RACF LIST commands are available:

LISTDSD List the details of one or more discrete or generic DATASET profiles, including the users and groups authorized to access the data set. See Figure 1 for a sample output.

LISTUSER List the details of one or more user profiles, including all the groups to which each user is connected.

LISTGRP List the details of one or more group profiles, including the users connected to the group.

RLIST List the details of discrete or generic profiles for one or more resources whose class is defined in the class descriptor table.

Before you can issue a RACF command, you must be defined to RACF with a sufficient level of authority. Refer to *RACF Command Language Reference* for a complete overview of the RACF commands and the authorities that are needed.

You can enter RACF LIST commands directly in the foreground during a TSO terminal session or by using RACF ISPF panels, and in the background by using a batch job. Entering RACF commands under TSO is faster than being lead

through the RACF ISPF panels. For the inexperienced user the RACF ISPF panels are still the recommended path to take. To see the on-line help for a command, enter, for example, HELP LISTUSER. From the panels, you can press the HELP key to display brief descriptions of the fields on the panels.

```
 LD DA('PAY.DATA.*') AUTHUSER DSNS
INFORMATION FOR DATASET PAY.DATA.* (G)

LEVEL  OWNER    UNIVERSAL ACCESS   WARNING   ERASE
-----  -------- ----------------   -------   -----
 00    PAYRES          NONE          NO      NO

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

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

YOUR ACCESS  CREATION GROUP  DATASET TYPE
-----------  --------------  ------------
   ALTER        SYS1           NON-VSAM

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

NO INSTALLATION DATA

              SECURITY LEVEL
-----------------------------------------
NO SECURITY LEVEL

CATEGORIES
----------
NO CATEGORIES

SECLABEL
--------
NO SECLABEL

   ID     ACCESS
--------  -------
PAYCLK     READ
PAYMST    UPDATE
PO01      UPDATE

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

DATA SETS AFFECTED BY PROFILE CHANGE
------------------------------------
PAY.DATA.INPUT
```

Figure 1. RACF Command Output

You can enter RACF commands in the background by submitting a batch job as follows:

```
//jobname  JOB  .....................
//STEP1    EXEC  PGM=IKJEFT01,DYNAMNBR=20
//SYSTSPRT DD    DSN=user.RACF.CMDOUT,DISP=SHR
//SYSTSIN  DD    *
 LD DA('PAY.DATA.*') AUTHUSER DSNS
/*
```

The output of this RACF command is displayed in Figure 1. The output of this sample job is stored in the pre-allocated data set that is specified in //SYSTSPRT.

The auditor should pay attention to the AUDITING specification (FAILURES(READ)), the GLOBALAUDIT specification, and the access list. Also note that the command output tells you what data sets are protected by the listed profile.

2.2 RACF SEARCH Command

The RACF SEARCH command is very powerful. With this command you can make real time inquires into the RACF database. The output of the command is listed directly on your terminal or used to construct a CLIST that is executed after the SEARCH command has completed. Before you can issue a SEARCH command, you must be defined to RACF with a sufficient level of authority.

The SEARCH command has numerous options and will not be covered in this document. If you need more information, refer to *Expanding the Capabilities of the RACF SEARCH Command*. The most frequently used feature of the SEARCH command is the CLIST option. You can make an inquiry of the current RACF database and, because this, build a CLIST for execution. For example, if you wanted to change the universal access of all your data set profiles, you would execute these two commands in sequence:

```
SEARCH NOMASK CLASS(DATASET) GENERIC CLIST('ALTDSD ','GENERIC UACC(NONE)')
EXEC EXEC.RACF.CLIST
```

This would search the RACF database for all data set profiles starting with your user ID and then build an ALTDSD RACF command for each data set profile found. You then need only execute the CLIST, and the universal access would be changed to NONE for every dataset profile.

One of the SEARCH command's few disadvantages is that it will execute only against the active primary RACF database. For example, if you have the system SPECIAL attribute, you can list all the profiles that a user has access to by issuing the following command:

```
SEARCH NOMASK USER(user ID)
```

The problem with this is that the user ID must be valid. In other words, you cannot search the RACF database for occurrences of a user ID, even if it were left on multiple access lists, as long as there is no valid user profile for that user ID. There can also be a performance impact if a SPECIAL user does an extensive search of the RACF database during prime shift. The solution is to run these commands in batch during off-shift hours.

2.3 RACF Cross Reference Utility - IRRUT100

RACF supplies a utility, IRRUT100 , that uses the RACF manager to search the RACF data base for all occurrences of a user ID or group name. IRRUT100 has been around a long time with very little change, apart from the occasional PTF. IRRUT100 issues a reserve for each profile read, and must be run against an active RACF database.

The strength of the utility is its ability to scan the RACF database for groups, or user ID′s supplied to the program by an authorized user. As with most programs, simplistic input normally means simplistic output.

To use the IRRUT100, you require one of the following attributes:

- SPECIAL
- group-SPECIAL
- AUDITOR
- group-AUDITOR

If you have none of these RACF user attributes, the job will still run, but only your own user ID will be listed. You cannot decentralize this function unless you give the submittor the required level of RACF user authority. This is further restricted by the user′s scope-of-group.

The output from IRRUT100 is either printed or written to a data set for further manipulation. Figure 2 gives an example of the output from the IRRUT100 utility. IRRUT100 would find the following group occurrences, among others:

- The group name, as it exists in the RACF database.
- The group is a subgroup of group xx.
- The group is a superior group of group xx.
- The group is the default group for user xx.
- The group is a connect group for user xx.
- The group name is the high-level qualifier of data set profile xx.
- The group has standard access to data set profile xx.
- The group is the owner of data set profile xx.

For user IDs, IRRUT100 provides information on the following occurrences:

- The user ID, as it exists in the RACF database.
- The user is a member of (connected to) group xx.
- The user is the owner of data set profile xx.
- The user has standard access to data set profile xx.
- The user has standard access to general resource xx.
- The user is to be notified when access violations occur against data set xx.
- The user is to be notified when access violations occur against general resource xx.
- The user is the resource owner of profile xx.

The problem with this utility is that all it does is to identify the occurrences of the user ID or group and nothing else. To manipulate the references, you have to

put the output into a data set and add RACF DELETE and REMOVE commands yourself.

There are some other issues as well, such as a certain performance impact. Let's look at performance first.

The perceived problem with IRRUT100 is that the RACF manager will enqueue on each RACF profile when checking to see whether the supplied group or user ID is found. In a large database during prime shift, this could create a potential performance problem for tasks that also need to enqueue on the RACF database. It is strongly recommended that IRRUT100 be run only off-shift. You should also try to search for all user IDs and group names in a single job (you can specify up to 1000 names), since you will still only enqueue once for every RACF profile (and the scanning for multiple names is negligible).

As you can see, IRRUT100 is a powerful utility but must be used with judgement so as not to affect performance in a negative way. The output will mostly need further processing before it is presented to a nonexpert.

```
Occurrences of IBMUSER

In standard access list of general resource profile TSOAUTH  RECOVER
Owner of TSOAUTH  RECOVER
In standard access list of general resource profile TSOAUTH  OPER
Owner of TSOAUTH  OPER
In standard access list of general resource profile TSOAUTH  JCL
Owner of TSOAUTH  JCL
In standard access list of general resource profile TSOAUTH  ACCT
Owner of TSOAUTH  ACCT
In standard access list of general resource profile PERFGRP  98
Owner of ACCTNUM  ACCNT#
In standard access list of general resource profile TSOPROC  IKJACCNT
Owner of TSOPROC  IKJACCNT
Owner of SECLABEL SYSNONE
Owner of SECLABEL SYSLOW
Owner of SECLABEL SYSHIGH
In standard access list of dataset profile SYS1.UADS
Owner of connect profile OPERHSM/SYS1
Owner of connect profile IBMUSER/VSAMDSET
Owner of connect profile IBMUSER/SYS1
Owner of connect profile IBMUSER/SYSCTLG
In access list of group VSAMDSET
Owner of group VSAMDSET
In access list of group SYS1
Owner of group SYS1
In access list of group SYSCTLG
Owner of group SYSCTLG
Owner of user OPERHSM
Owner of user IBMUSER
User entry exists
Owner of user DON
```

Figure 2. Sample IRRUT100 Output

2.4 REXX Programs

RACF has a large amount of information stored in its database, but unfortunately it is not easy to extract. There are utilities and commands that interrogate the database, but the output has never been quite the way the common user would like to see it.

To present this data in a more meaningful way, the RACF administrator had to learn either Assembler and macro programming, or one of the more modern programming/command languages such as REXX (on VM and MVS) or CLISTs (MVS only). You may even want to combine Assembler programs and REXX procedures.

Although Assembler programs are very powerful, they require a high level of skill and an understanding of the RACF database structure. The only advantage is that you could interrogate every field in the entire RACF database. All this must be done on live RACF databases; we cannot use copies of the database since the Assembler macros used to read the RACF database only work on the live databases; copies and backups cannot be used.

Today, most administrators rely on REXX EXECs to manipulate RACF output. The usage of the modern programming/command languages, such as REXX (on VM and MVS) or CLISTs (MVS only), are the easiest to use since they are easy to learn and can easily manipulate output data like that from a RACF command. Changes are made and tested without recompiling. These modern languages are also easy to debug.

The only problem is that you must provide input that the EXEC can use; for example, the output from IRRUT100 or even the output from a RACF command like that in Figure 1 on page 4. This means that if you choose IRRUT100, you must run it before executing a CLIST or REXX program. Remembering that IRRUT100 can affect performance of the system, this is not a good idea unless it is done after prime shift.

2.5 RACF Database Unload Utility

After RACF 1.9 became generally available, a Small Programming Enhancement (SPE) was announced - the *RACF Database Unload Utility*, IRRDBU00. This utility reads a RACF database, either the primary or a copy, and creates a sequential data set. This data set can be:

- Sorted
- Used as input to an installation-written program
- Manipulated by REXX EXECs or CLISTs
- Loaded into a relational database such as DB2 or SQL/DS*

Note: Once the data has been unloaded, the end-user has access to most of the information stored in the RACF database, except for passwords and some RACF system options. This means that the unloaded data should have the same level of protection as your primary RACF database.

You will also need UPDATE access to the RACF database when executing IRRDBU00.

Samples of how to use this new function are included in SYS1.SAMPLIB.

The samples also show how the output of the RACF Database Unload Utility are loaded into DB2 tables, sorted by record type, or even manipulated by REXX commands or CLISTs. The preferred way is to load the data into DB2 tables and then use QMF or SQL queries to perform adhoc queries on the data. Refer to Figure 3 for a sample query.

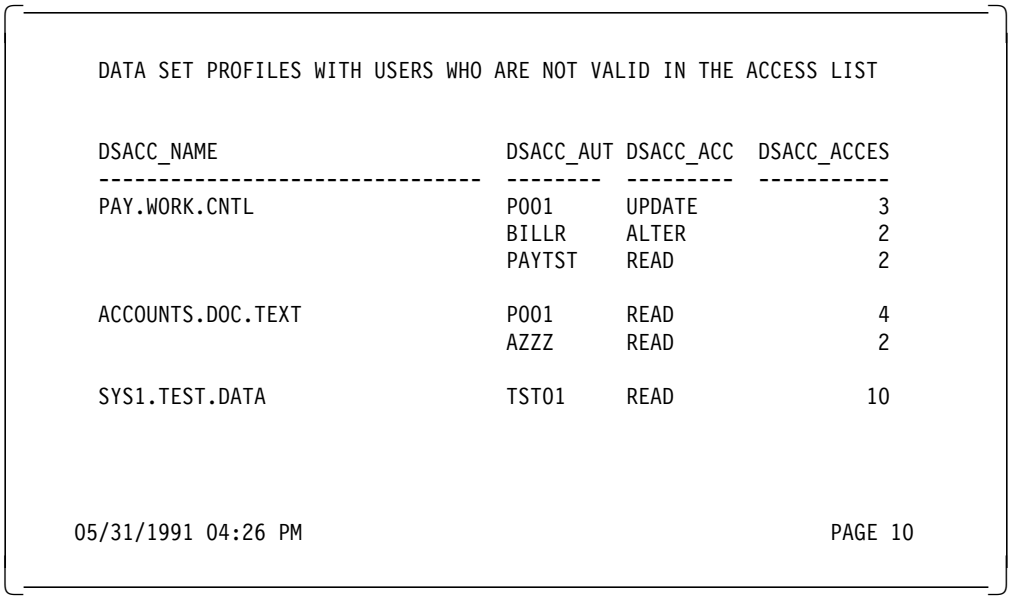
```
Description: Check all of the data set standard access lists and
             verify that each user ID is a valid user or
             group ID

Tables Accessed: SQL
                 |DS_ACCESS|     - A list of dataset authorities
                 |AUTH_IDS|      - A list of valid user/group IDs


SELECT
                  DSACC_NAME
                 ,DSACC_AUTH_ID
                 ,DSACC_ACCESS
                 ,DSACC_ACCESS_CNT
           FROM
                 USER01.DS_ACCESS X
           WHERE NOT EXISTS
                 ( SELECT *
                    FROM
                         USER01.AUTH_IDS
                    WHERE
                    X.DSACC_AUTH_ID=AUTHID_NAME
                      )
             ORDER BY 1
             ;
```

Figure 3. Sample SQL Query

Figure 4 shows the results from the SQL query.

Note: Not all resulting rows are shown.

By changing the SQL statement slightly, you could produce the necessary RACF commands to clean up the RACF database directly.



DATA SET PROFILES WITH USERS WHO ARE NOT VALID IN THE ACCESS LIST

DSACC_NAME	DSACC_AUT	DSACC_ACC	DSACC_ACCES
PAY.WORK.CNTL	P001	UPDATE	3
	BILLR	ALTER	2
	PAYTST	READ	2
ACCOUNTS.DOC.TEXT	P001	READ	4
	AZZZ	READ	2
SYS1.TEST.DATA	TST01	READ	10

05/31/1991 04:26 PM PAGE 10

Figure 4. Sample Report

2.6 RACF Report Writer

The *RACF Report Writer* (RACFRW) lists the contents of the System Management Facilities (SMF) records in a format that is easy to read. You can tailor the reports to select only SMF records for specific RACF log information.

With the RACF Report Writer, you can obtain:

- Reports that describe attempts to access RACF protected resources in terms of user name, user identity, number and type of successful accesses, and number and type of attempted security violations
- Reports that monitor the use of RACF commands
- Reports that describe specific user and group activity
- Reports that monitor SPECIAL and OPERATIONS users
- Reports that monitor password violations
- Reports that summarize system use and resource use

The RACF Report Writer consists of three phases:

- Command and subcommand processing
- Report selection
- Reports generation

Command and subcommand processing starts when you enter the TSO command RACFRW or run the report writer as a batch job. You can specify the RACF Report Writer subcommands SELECT, EVENT LIST, SUMMARY and END. The SELECT and EVENT subcommands specify which input records the RACFRW should select to generate the report. The reports are formatted by using the LIST subcommand to list each SMF record you select and the SUMMARY subcommand to format and print a summary listing of the selected SMF records.

The RACF Report Writer compares each record from the SMF data file against the criteria you specify on the SELECT and EVENT subcommands. Only the records that match your selection criteria are processed, creating reports.

RACF Report Writer formats the report according to the specifications in the LIST and SUMMARY subcommand.

Three reports show sample output from the RACF Report Writer.

A Listing of options set in the RACF installation is shown in Figure 5, the RACF Report Writer Listing of Status Records.

```
90.053 13:51:40              RACF REPORT - LISTING OF STATUS R ECORDS

DATE   TIME     SYSID MISC. OPTIONS      EXITS    CLASS    PROT  STAT AUD GEN GCMD GLBL GLST RLST LOPT
90.053 12:17:41 R19O  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' ACC ESS CHECKING IS ACTIVE
                                            SINGLE LEVEL NAMES N OT ALLOWED
                                            INTERVAL:  253 DAYS
                                            HISTORY:  NONE
                                            REVOKE:   NO
                                            WARNING:  NONE
                                            INACTIVE:   NO
                                            NO PASSWORD SYNTAX R ULES
                                          SECURITY OPTIONS:
                                            SECLABELCONTROL: INA CTIVE
                                            CATDSNS:         INA CTIVE
                                            MLQUIET:         INA CTIVE
                                            MLSTABLE:        INA CTIVE
                                            MLS:             INA CTIVE
                                            MLACTIVE:        INA CTIVE
                                            GENERICOWNER:    INA CTIVE
                                            SECLABELAUDIT:   INA CTIVE
                                            COMPATMODE:      INA CTIVE
```

Figure 5. RACF Report Writer - Listing of Status Records

In Figure 6, we can see the RACF Report Writer User Summary Report.

89.196 14:23:38 RACF REPORT - SHORT USER SUMMARY

USER/ *JOB	NAME	JOB/LOGON SUCCESS	JOB/LOGON VIOLATION	RESOURCE STATISTICS SUCCESS	RESOURCE STATISTICS WARNING	RESOURCE STATISTICS VIOLATION	INTENTS ALTER	INTENTS CONTROL	INTENTS UPDATE	INTENTS 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
b											
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 6. RACF Report Writer - Short User Summary Report

The resource access by users is shown in Figure 7, the RACF Report Writer Resource by User Summary Report.

You can write your own post-processor programs to do additional processing on the RACF Report Writer output.

Note: As mentioned in the *RACF Auditors Guide*, the RACF Report Writer is no longer the IBM-recommended utility for processing RACF audit records. The report writer supports existing audit records for releases prior to 2.1. It does not support most of the audit records introduced for the new functions in 2.1.

```
89.218 12:36:12                          RACF REPORT - RESOURCE BY USER SUMMARY
      USER/                                                  ------------ I N T E N T S ------------
      *JOB                                  SUCCESS   WARNIN G 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 7. RACF Report Writer - Resource by User Summary Report

2.7 RACF Data Security Monitor

The *RACF Data Security Monitor* (DSMON) allows an authorized user to produce reports on the options and access controls that affect system integrity in your operating system.

DSMON produces the following reports:

- System report
- Group tree report
- Program Property Table (PPT) report
- RACF authorized caller table report
- RACF Class Descriptor Table (CDT) report
- RACF exits report
- RACF Global Access Checking (GAC) report
- RACF Started Procedure Table (SPT) report
- Selected user attribute summary report
- Selected data sets report

DSMON is a program that normally should run while RACF is active. It runs as an authorized program facility (APF) authorized batch program.

You must either have the AUDITOR attribute to run the DSMON or must have READ authority to the profile that protects DSMON as a program module.

Refer to the *RACF Auditors Guide* for a complete overview of the usage of the DSMON.

2.8 RACF SMF Data Unload Utility

The *RACF SMF Data Unload Utility* is a new facility in RACF 2.1 that allows installations to create a sequential file from the security relevant audit data. The sequential file is used in several ways:

- Viewed directly
- Used as input for installation written programs
- Manipulated with sort/merge utilities
- Loaded into a relational database manager (for example DB2)
- Downloaded to a workstation for the use with various workstation programs

The RACF SMF Data Unload Utility is implemented in the form of exits USER2 and USER3 for the *SMF Dump Utility* (IFASMFDP). The corresponding module names are IRRADU00 and IRRADU86 respectively.

Figure 8 shows a sample JCL to invoke the RACF SMF Data Unload Utility. Refer to the *RACF Macros and Interfaces* for more information.

```
//USER01   JOB Job card
//UNLOAD   EXEC PGM=IFASMFDP
//DUMPIN   DD   DISP=SYS1.MANA
//DUMPOUT  DD   DUMMY
//OUTDD    DD   DISP=OLD,DSN=USER01.SMF.IRRADU00
//ADUPRINT DD   SYSOUT=*
//SYSRINT  DD   SYSOUT=*
//SYSIN    DD   *
//  USER2(IRRADU00)  USER3(IRRADU86)
//      DATE(94210)
//      START(0800)
//      END(1700)
//      SIS(SYS1)
/*
```

Figure 8. Sample JCL to Invoke the SMF Data Unload Utility

There are two members in the SYS1.SAMPLIB dataset that show how to define DB2 tables and how to load RACF SMF Data Unload Utility data into these tables. There is also a member with some samples to do SQL queries to the SMF data tables.

2.9 SystemView Enterprise Performance Data Manager/MVS

Even if it is not normally used by RACF auditors, you should be aware that the *IBM SystemView Enterprise Performance Data Manager/MVS* (EPDM) program product also provides reports on SMF records written by RACF.

EPDM is a product for collecting performance data, summarizing it, and saving it in a DB2 database.

EPDM has two basic functions:

- Collecting systems management data into a DB2 database
- Reporting on the data

EPDM can generate graphic and tabular reports using systems management data it stores in its DB2 database.

EPDM gets performance data about systems from various log data sets, such as the System Management Facilities (SMF) log dataset in MVS or from the Information Management System (IMS) log dataset.

Once SMF data has been stored in the EPDM database, the EPDM reporting dialog lets you report on the data in a variety of formats. When you use the reporting dialog to display or print a report, EPDM runs a corresponding QMF query to retrieve data from the database, and to display or print the results as specified in the associated QMF form.

Since you can specify to EPDM the SMF records to be used for reporting, you can also specify that you want reports for the three RACF related SMF records:

- RACF processing (SMF record type 80)
- RACF initialization (SMF record type 81)
- RACF audit record for data sets (SMF record type 83)

There are several RACF related reports predefined in EPDM.

- RACF AUDITOR user commands - auditor report
- RACF command failures - auditor report
- RACF logon/job failures
- RACF OPERATIONS user access - auditor report
- RACF resource access failures
- RACF resource accesses
- RACF SPECIAL user commands - auditor report
- MVS jobs with RACF S913 ABENDs

You can naturally create your own reports using QMF.

Refer to the *EPDM General Information* and to *EPDM Administration Guide* for more information.

Figure 9 shows the EPDM selection panel with the RACF related reports you can select.

```
  Report  Batch  Group  Search  Options  Other  Help
------------------------------------------------------------------------
                              EPDM Reports              ROW 277 TO 288
Command ===> ____________________________________________________________

Select a report. Then press Enter to display.

Group  . . . . . : All reports

/  Report                                                  ID
_  MVS Jobs with RACF S913 Abends, Daily                   MVS54
_  RACF AUDITOR User Commands - Auditor Report             RACF04
_  RACF Command Failures - Auditor Report                  RACF02
_  RACF Logon/Job Failures                                 RACF01
_  RACF OPERATIONS User Access - Auditor Report            RACF05
_  RACF Resource Access Failures                           RACF06
_  RACF Resource Accesses                                  RACF07
_  RACF SPECIAL User Commands - Auditor Report             RACF03
```

Figure 9. RACF Related Reports on the EPDM Selection Panel

Two sample reports from EPDM are shown. Figure 10 shows the resource access failure report.

```
                                    RACF Resource Accesses Failure
                                      System: R.SYSTEM_ID
                                Date: DATE(1994-08-16) to DATE(1994-08-16)
                                   Minimum security level: 0


Responsible          Sec-  Resource                       Gen- User     Access  Access
   user     Class    level   name                         eric  ID      request allowed Date
----------- -------- ----- ------------------------------ ---- -------- ------- ------- ----------
USER02      DATASET  0     USER02.DSN                     Y    USER01   UPDATE  NONE    1994-08-16
USER04      DATASET  0     USER04.DSN                     Y    USER01   UPDATE  NONE    1994-08-16
SYSPRG      DATASET  0     SYS1.PARMLIB                   Y    USER02   READ    NONE    1994-08-16
SYSPRG      DATASET  0     SYS1.PARMLIB                   Y    USER03   READ    NONE    1994-08-16
USER02      DATASET  0     USER02.DSN                     Y    USER03   UPDATE  READ    1994-08-16
USER02      DATASET  0     USER02.DSN                     Y    USER01   UPDATE  NONE    16.08.94




                                        EPDM Report: RACF06
```

Figure 10. EPDM Resource Access Failure Report

Figure 11 shows a report of MVS jobs that produced RACF S913 ABENDs (insufficient access authority).

MVS Jobs with RACF S913 Abends, Daily
Date: DATE(1994-08-16) to DATE(1994-08-16)

MVS system id	User group	RACF userid	Account field1	Date	Time	Job name
1120	GROUP1	USER01	-	1994-08-16	11:15:09	TAPE01
	GROUP1	USER02	-	1994-08-16	15:08:15	UNLTAPE
	GROUP2	USER03	-	1994-08-16	09:46:59	JOB001
		USER04	-	1994-08-16	11:37:18	JOB723
	GROUP2	USER02	-	1994-08-16	12:28:25	BACKUP
		USER05	ACC02	1994-08-16	12:31:46	JOB023
	GROUP1	USER01	-	1994-08-16	12:04:15	JOB123

EPDM Report: MVS54

Figure 11. EPDM Report of MVS Jobs That Produced RACF S913 ABENDs

Chapter 3. The Auditing Application

This chapter discusses an *auditing application* and the steps necessary to install it at a customer site. Refer to 1.1, “How to Order Materials Discussed in This Document” on page 2 for information on how you may obtain a copy of the auditing application.

3.1 Description of the Auditing Application

The auditing application is based on the Interactive System Productivity Facility (ISPF) and guides the auditor through a set of panels. The panels offer predefined reports and the means of limiting the amount of output data. The object of auditing being to find the things that are unusual, there are selections to allow only violations to be viewed or to study all the events that took place during a narrow window of time.

The reports that are shown are the result of REXX programs which are invoked as the result of the selections made. The Query Management Facility (QMF) is used as the query manager software to execute queries and to format the output.

The auditing application uses data extracted from the System Management Facility (SMF) datasets to build its reports. However, the data as logged in the SMF datasets is not directly usable to QMF, but must first be unloaded by the RACF SMF Data Unload Utility and then loaded into the DB2 format. The necessary steps are documented in the *RACF Auditor's Guide*.

3.2 Prerequisites for the Auditing Application

The auditing application requires the following products to work.

RACF 2.1

ISPF/PDF

TSO/E V2 (for REXX support)

DB2 Version 2 Release 3 or later

QMF Version 3 Release 1.1 or later

You may be able to use older versions of DB2, but we have not tested the auditing application using other versions of the above program products. For QMF, you need the Version 3 Release 1.1, since this is the first release that included the REXX callable interface.

The installation of the auditing application does not require any modifications to be done to your operating system or the RACF database.

3.3 Installing the Auditing Application

The application consists of the following data sets:

userid.RACF.EXEC

userid.RACF.PANELS

userid.RACF.EXP.DATA

userid.RACF.QUERY

userid.RACF.PROC

userid.RACF.FORM

The ***userid***.RACF can be replaced with whatever qualifiers you prefer. Having received these data sets on your system, you are ready for the following steps:

1. Modify your TSO/ISPF LOGON procedure or allocation command list to include the EXEC data set and the PANELS data set. The PANELS data set is concatenated before your other panel data sets. The procedure used as a basis should have the necessary data sets and specifications to allow you to run DB2 and QMF.
2. The *auditing application base panel* RACF01 (Figure 12) is the base panel from which you chose the reports you wish to run. You start the application by whatever selection your installation has chosen.

```
                              RACF reporting
 ===> ____________________________________________________________

  1 - User based reports
  2 - Group based reports
  3 - Profiles based on UACC
  4 - Profile information

  5 - Compressed general resource report
  6 - Compressed user profile report
  7 - Compressed group profile report
  8 - Compressed data set profile report

  9 - Groups and connected users
 10 - Users and their connect groups
 11 - All occurrences of a userid or group name
 12 - Access list clean-up

  A - Audit reports
  Q - QMF -- Query Management Facility


  0 - Updating user parameters
```

Figure 12. Auditing Application Base Panel - RACF01

3. On the RACF01 panel, enter the **INSTALL** command which will take you to the RACFIMPO panel shown in Figure 13. On this panel, enter the names of the EXP.DATA, QUERY, PROC, and FORM data sets that you have just received.

The default assumption is that your data sets have names where the high level qualifier is equal to your own user ID, and the second qualifier is equal to RACF. If these assumptions are correct, then just enter **IMPORT** on the command line and press Enter. The import of the necessary QMF objects will now start. If you have chosen other names for your data sets, please fill in those names instead in addition to the import, and press Enter.

Note: The alternate names have to be entered in quotes and fully qualified, including the ending DATA, QUERY, PROC, and FORM.

```
                        RACF EXPORT / IMPORT
===> ____________________________________________________________________
     _

EXP.DATA data set:  RACF.EXP_____________________________________
QUERY    data set:  RACF_________________________________________
PROC     data set:  RACF_________________________________________
FORM     data set:  RACF_________________________________________
```

Figure 13. RACFIMPO Panel

4. When the QMF IMPORT starts, you will see messages on your terminal telling you what objects are being imported. If you do not receive these messages, or if you get error messages, try correcting the errors if you can, or contact someone who can help you. After the IMPORT is done, you will be back at the RACFIMPO panel and should now press PF3 to return to the base panel. Your next choice on the base panel should be selection “0” to update your user parameters. The panel ID is RACFPARM and is shown in Figure 14.

```
                              RACF reporting
 ===> ____________________________________________________________

 DB2 subsystem ID  :  DB23__

 RACF Database report

 QMF proc. creator :  ASKO___       Prefix of QMF procedures
 RACF table creator:  GEORGE_       Prefix of DB2 tables

 RACF Audit report

 QMF proc. creator :  ASKO____      Prefix of QMF procedures
 RACF table creator:  USER01__      Prefix of DB2 tables

 QMF / PDF
 Data interchange  :  TEMPFILE_____________________________
 Report browsing      QMF____       QMF or BROWSE for ISPF browse

Change your profile information and use PF3 to return
```

Figure 14. RACFPARM Panel

Please update the parameters with relevant information for your installation. If you have done the INSTALL step, your user ID should be entered as the QMF procedures creator for the both the RACF database reports and the RACF audit reports. The prefix for the databases that are created by the RACF Database Unload Utility and the RACF SMF Data Unload Utility respectively do not necessarily have to be the same.

The installation defaults for the default QMF procedure creator user IDs, the default DB2 table creator user IDs, and the DB2 subsystem name is found in the "***userid***.RACF.EXEC" data set in member RACFSQMF. This REXX EXEC is used to start the QMF interface. The values to be changed are found at the beginning of the EXEC and are marked by "????" for easy reference.

The report browsing option, shown at the bottom of panel RACFPARM, has the value of QMF for using normal QMF output and BROWSE to use ISPF BROWSE instead. Using ISPF BROWSE makes the response times a little longer, but has the advantage of letting you use FIND commands, which are not possible using normal QMF output.

5. Having finished the above steps, you are ready to start using the reporting application.

3.4 Installing ISPF Panels and REXX Programs

Depending on your installation standards, you will either be using many LOGON procedures that are dedicated to given applications, or you have a few procedures where you use CLISTs to allocate the necessary data sets.

Appendix A, "Sample CLIST for Starting the Report Application" on page 61, provides an example of a CLIST that is used to allocate the necessary data sets for our reporting application. The CLIST name (DB23RACF) is given as the first command to be executed on your LOGON panel, or it could be given from a TSO READY prompt.

Your ISPF primary panel has to be changed to include selections for the application, and the "userid.RACF.PANELS" library contains member DB23PRIM that includes the "rr" and "rrr" selections. Both the "rr" and "rrr" selections take you to the RACF01 panel, the difference being that the "rr" selection starts QMF before showing the RACF01 panel. The "rrr" selection goes directly to the RACF01 panel, and QMF is started when you enter a report selection.

You will have to either modify your own standard primary panel to include these selections or make them available by including the supplied DB23PRIM panel in the ISPPLIB concatenation.

For the DB23RACF CLIST to be executed when entered from the LOGON panel or a READY prompt, it must be installed in one of the libraries concatenated under your SYSPROC DD card in your LOGON procedure.

All the other REXX procedures that are used by the reporting application are found in the "userid.RACF.EXEC" library.

3.5 Installing the QMF Part of the Report Application

The QMF files that you get with the application are EXPORT copies of the QUERY, PROC, and FORM libraries and the EXP.DATA data set, used to control the installation process. These data sets are used when you specify **INSTALL** on the primary panel of the application. INSTALL will IMPORT the objects into your system, making them available for use when running the application.

The REXX language interface used in the application is available only with QMF Version 3 Release 1.1 or later; therefore, if you do not have this release installed, you cannot run the application as it is.

QMF lets you use the PF key that has been defined as you “print” key to print the reports that you are producing. The CLIST in Appendix A, “Sample CLIST for Starting the Report Application” on page 61, shows you a sample allocation for the DSQPRINT data set for printing reports to SYSOUT. Your installation can also define the print function to allow reports to go directly to specific printers.

Chapter 4. Using the Auditing Application and Sample Reports

This section describes how to use the auditing application and the various reports that you can obtain.

4.1 Loading the Actual SMF Data

Before you start producing reports you should run the RACF SMF Data Unload Utility to unload your SMF data and load it into DB2 tables. For most installations it will be acceptable to do an SMF unload once a day, for example as a batch job during the night. Most installations have already automated their procedure for dumping the SMF data so that the datasets are either dumped during the night or when they become full. The auditor data will, therefore, have to be extracted from these dumps by running the RACF SMF Data Unload Utility against them.

4.2 Selecting Reports

The *audit reports main panel* for the auditing application is shown in Figure 15. You reach this panel by selecting **A - Audit reports** from the *auditing application base panel* shown in Figure 12 on page 20.

```
                              Audit Reports
===> ____________________________________________________________


 SMF system id:   ____
 Start date:      __________     End date:  __________
 Start time:      __________     End time:  __________


        Only the violations:  ___   (YES/NO)


 1 - Summary of events
 2 - Access to a specific resource
 3 - Events by a specific user
 4 - Events due to special attributes or logging options
```

Figure 15. Audit Reports Main Panel

The audit reports main panel has the following major sections:

- Summary of events
- Access to a specific resource
- Events by a specific user
- Events because of special attributes or logging options

Whenever you specify names in an input field on the panels of the auditing application, you have to remember that QMF is used as a query manager. The percent sign (%) is used as a generic character and not the asterisk (*), which is often the case.

Names can either be fully qualified names or generic names, the latter meaning you give just a part of the name. You can also specify that you want all names that contain a given set of characters, such as %LINK% (will select both SYS1.LINKLIB and PLI.SYMLINK). Specifying, for example SYS1, will be expanded into SYS1% by the application. In other words, all the names you specify will be considered generic.

4.2.1 Limiting the Amount of Data

Depending on the audit options set in RACF, many SMF records might be produced. To limit the amount of data produced for specific auditing reports, all panels allow you to specify the system ID, the dates and the times.

System: If SMF records are written by more than one system, you can select only events for a specific system by specifying the SMF-ID of this system. If no SMF-ID is specified, events from all systems are selected.

If you do not know the SMF-ID, the RACF Data Security Monitor (DSMON) will list it for you in the *System Report*.

Date: You can specify a start date and an end date to get output for a specific date or a specific period. The allowable formats are:

ISO JIS	yyyy-mm-dd	1994-08-23
USA	mm/dd/yyyy	08/23/1994
Europe	dd.mm.yyyy	28.08.1994

If no date is specified, all the records loaded into the RACF SMF DB2 tables are processed.

Time: You may specify a start time and an end time to limit the output to a particular time window. The allowable formats are:

ISO	hh.mm.ss	09.30.00
USA	hh:mm:AM	09:30:AM
Europe	hh.mm.ss	09.30.00
JIS	hh:mm:ss	09:30:AM

If no time is specified, all records provided by the RACF SMF Data Unload Utility are processed.

4.2.2 Access Violation Reports

Auditors are primarily interested in seeing reports on access violations. On the audit reports main panel and on all the other auditing panels, you can specify that you want reports for access violations only or that you want all accesses.

If you specify **yes** on the panels, you will get violation reports only. Specifying **no** or blank will result in all events being included into the report.

4.2.3 Summary of Events

A summary of all RACF events is obtained by selecting option **1 - Summary of events** on the audit reports main panel. The resulting report is shown in Figure 16.

```
                        RACF AUDIT Summary                      ROW 1 TO 14
 ===> ____________________________________________________________________

Select an event from the following list:

      Event
Sel   Type        Qualifier          Count          Violation

_     ACCESS      INSAUTH               14          YES
_     ACCESS      SUCCESS             3427
_     ADDSD       SUCCESS                1
_     ADDVOL      SUCCESS               10
_     ALTUSER     SUCCESS                2
_     DEFINE      SUCCESS              348
_     DELRES      SUCCESS              364
_     JOBINIT     INVPSWD                7          YES
_     JOBINIT     PWDEXPR                2          YES
_     JOBINIT     RACINITD               4
_     JOBINIT     RACINITD               3
_     JOBINIT     SUBNATHI               2
```

Figure 16. Event Summary Report

All events of a given type and the event qualifier for these events along with the number of such events are listed. Any event type which involves one or more violations is indicated by a highlighted ″YES″ in the ″Violation″ column.

This list gives you an overview of what kind of events have taken place in the specified time range. The *RACF Macros and Interfaces* lists all events types and also lists all possible event qualifiers.

The *RACF AUDIT Summary* report is used for further processing.

By entering an **S** in the selection column (Sel), you will get a detailed list about this event type including the user ID that caused the event, the event type, the event qualifier and the resource name. A sample report is shown in Figure 17.

```
                                EVT
EVENT      EVENT                USER       DATE        TIME      RES
TYPE       QUAL       TERM       ID       WRITTEN     WRITTEN   NAME
---------  ---------  ---------  --------  ----------  --------  --------- --------
ACCESS     INSAUTH    A4F8X403   USER01    08/16/1994  05:00 PM  SYS1.PARMLIB
ACCESS     INSAUTH    A4F8X403   USER02    08/16/1994  05:00 PM  JES2.CANCEL.BAT
ACCESS     INSAUTH    DDJ8F301   USER04    08/16/1994  05:32 PM  USER01.DAT
ACCESS     INSAUTH    DDJ8F301   USER01    08/16/1994  05:32 PM  USER04.DAT
ACCESS     INSAUTH    DDJ8F301   USER10    08/16/1994  05:33 PM  USER01.DAT
ACCESS     INSAUTH               USER01    08/16/1994  05:33 PM  SBMVS.D.BAT
ACCESS     INSAUTH               USER05    08/16/1994  05:33 PM  SBMVS.D.BAT
ACCESS     INSAUTH               USER05    08/16/1994  05:33 PM  SBMVS.D.B AT
ACCESS     INSAUTH    DDJ8F301   USER01    08/16/1994  05:33 PM  JES2.CANEL.BAT
ACCESS     INSAUTH    DDJ8F301   USER01    08/16/1994  05:33 PM  SYS1.PARMLIB
```

Figure 17. Detailed Event List

By entering an **U** into the selection column, you will get a detail report of the users that have caused the corresponding events.

By entering an **R** into the selection column, you will get a detail report of the resources involved in the corresponding events. A sample list is shown in Figure 18.

```
                        RACF AUDITOR RESOURCE REPORT

DAUDIT
ACCESS / INSAUTH

              DATE         TIME      RES
  TERM       WRITTEN      WRITTEN    NAME
  --------   ----------   --------   -------------------------------------
  SCGSQ119   08/16/1994   05:40 PM   SYS1.RACFEXIT
             08/16/1994   06:52 PM   SYS1.RACFCHK
  SCGSQ119   08/16/1994   06:59 PM   ISFCMD.ODSP.SYSLOG.JES2
  SCGSQ119   08/16/1994   06:59 PM   ISFCMD.ODSP.SYSLOG.JES2
```

Figure 18. RACF Auditor Resource Report

4.2.4 Access to Specific Resources

Reports of accesses to a specific resource are selected by option **2 - Access to a specific resource** on the audit reports main panel.

These reports may help you to find all violations against a specific resource and to find the user who caused the violation. It is also possible to monitor all accesses to a specific resource, providing the log options are set to log all accesses.

Option 2 takes you to the panel shown in Figure 19, where you can specify the name of the resources you are interested in.

```
            Audit Reports - Resource Name Selection
===> ____________________________________________________________


 SMF system id:   ____
 Start date:      __________     End date:  __________
 Start time:      __________     End time:  __________

       Only the violations:  ___   (YES/NO)

 Resource name:  ____________________________________
```

Figure 19. Resource Selection Panel

For each resource matching the selection criteria specified on the panel, you will see information about the access event type, the access event qualifier, the user ID of the user accessing the resource, the date and time of the access and if there was an access violation. A sample report is shown in Figure 20

```
SYS1.ADRDSSU

                    ACC
 ACC       ACC      EVT         ACC         ACC
EVENT     EVENT     USER       DATE        TIME        ACC
TYPE      QUAL       ID       WRITTEN     WRITTEN   VIOLATION
--------  --------  --------  ----------  --------  ---------
ACCESS    SUCCESS   USER01    16.08.1994  07.19.53  N
ACCESS    SUCCESS   USER02    16.08.1994  07.22.11  N
ACCESS    INSAUTH   USER03    16.08.1994  07.23.32  Y


SYS1.PARMLIB

                    ACC
 ACC       ACC      EVT         ACC         ACC
EVENT     EVENT     USER       DATE        TIME        ACC
TYPE      QUAL       ID       WRITTEN     WRITTEN   VIOLATION
--------  --------  --------  ----------  --------  ---------
ACCESS    INSAUTH   USER01    16.08.1994  06.29.53  Y
ACCESS    SUCCESS   USER03    16.08.1994  08.27.32  N
```

Figure 20. Access to Specific Resources

4.2.5 Events by a Specific User

Reports of events caused by a specific user are selected by option **3 - Events by a specific user** on the audit reports main panel. This report helps you to find all violations a user has caused in the specified time range. This report will also help you to monitor all activities of a specific user if the audit option is set for this user.

Option 3 takes you the a panel shown in Figure 21, where you can specify a user ID.

```
          Audit Reports - User ID Selection
===> ____________________________________________________________

 SMF system id:   ____
 Start date:      __________     End date:  __________
 Start time:      __________     End time:  __________

      Only the violations:  ___   (YES/NO)

 User ID:  ________
```

Figure 21. User Selection Panel

Figure 22 shows a sample report for a specific user ID. This report gives you an overview of the event types, the corresponding event qualifiers and the number of events caused by specific users. It also shows if there were any violations.

If no user ID is specified, an overview for all users is created. The user IDs are listed in alphabetic order.

To get more detailed information, you can use this report for further processing. Typing an **S** in the selection column (SEL) will get you a detailed list with more information, including the resource name and the date and time the event occurred.

```
                Event
Sel  Userid     Type      Qualifier    Count  Violation

_    USER01     ACCESS    INSAUTH          4  YES
_    USER01     ACCESS    SUCCESS         44
_    USER01     DEFINE    SUCCESS          4
_    USER01     JOBINIT   SUCCESS          2
_    USER01     JOBINIT   TERM             2
```

Figure 22. Specific User Report

4.2.6 Events Because of Special Attributes or Logging Options

Specifying option **4 - Events due to special attributes or logging option** on the audit reports main panel takes you to a panel shown in Figure 23, where you can get information about two different reasons of SMF logging.

```
       Audit Reports - Special Attributes and Logging Options
===> _____________________________________________________________

 SMF system id:   ____
 Start date:      __________     End date:  __________
 Start time:      __________     End time:  __________

        Only the violations:  ___   (YES/NO)

 Special attributes that                 Logging options
 allowed access:                         that caused logging:

 Auth. special: _  (Y/N)                 Class   : ___
 Auth. oper   : _  (Y/N)                 User    : ___
 Auth. audit  : _  (Y/N)                 Special : ___
                                         Access  : ___
```

Figure 23. Special Attributes and Logging Options Selection Panel

You can get a report about events where access has been granted because of the following RACF authorities:

- SPECIAL
- OPERATIONS
- AUDIT

Whenever an access is granted because of these attributes, an SMF record is written, providing the corresponding audit options are set.

Besides these records, an auditor can specify special audit options in SETROPTS to enforce SMF logging. For example, the auditor can log all activities for a specific user or all activities for a user with the RACF SPECIAL attribute.

You can get a report for the following audit options:

- Class
- User
- Special
- Access

Specifying a **Y** for one or more of the above selections will tell what events to include in the resulting report. If you make no selections at all, a report of all events will be produced.

The SPECIAL and OPERATIONS attributes are very powerful RACF authorities, and an auditor should carefully monitor the activities of these users.

You can get a list of all users with the SPECIAL, OPERATIONS or AUDIT attributes by specifying the *selected attributes report* using the DSMON.

You can also use DSMON to obtain which classes are defined in the class descriptor table and whether there is auditing for the specified class.

Whether you request a report about access because of a specific RACF authorization or because of specific audit option, the structure of the output is the same. A sample report for events logged because of the SPECIAL attribute is shown in Figure 24.

```
                  EVT
EVENT    EVENT    USER      DATE       TIME    VIO- AUTH.  LOG.
TYPE     QUAL      ID      WRITTEN    WRITTEN  LAT. S O A  C U S A
-------- -------- -------- ---------- -------- ---- ------ --------
ALTUSER  SUCCESS  USER02   08/16/1994 05:53 PM N    Y N N  Y N Y N
ALTUSER  SUCCESS  USER02   08/16/1994 05:53 PM N    Y N N  Y N Y N
PERMIT   SUCCESS  USER03   08/16/1994 05:54 PM N    Y N N  Y N Y N
PERMIT   SUCCESS  USER03   08/16/1994 05:55 PM N    Y N N  Y N Y N
ADDSD    SUCCESS  USER01   08/16/1994 06:11 PM N    Y N N  Y N Y N
DEFINE   SUCCESS  USER01   08/16/1994 06:11 PM N    Y N N  Y N N Y
PERMIT   SUCCESS  USER02   08/16/1994 06:11 PM N    Y N N  Y N Y N
PERMIT   SUCCESS  USER01   08/16/1994 06:23 PM N    Y N N  Y N Y N
PERMIT   SUCCESS  USER02   08/16/1994 06:23 PM N    Y N N  Y N Y N
PERMIT   SUCCESS  USER01   08/16/1994 06:49 PM N    Y N N  Y N Y N
PERMIT   SUCCESS  USER01   08/16/1994 06:49 PM N    Y N N  Y N Y N
PERMIT   SUCCESS  USER02   08/16/1994 06:49 PM N    Y N N  Y N Y N
PERMIT   SUCCESS  USER01   08/16/1994 06:49 PM N    Y N N  Y N Y N
PERMIT   SUCCESS  USER01   08/16/1994 06:49 PM N    Y N N  Y N Y N
PERMIT   SUCCESS  USER02   08/16/1994 06:49 PM N    Y N N  Y N Y N
```

Figure 24. Events Due to SPECIAL Attribute Report

The report shows the event type, the event qualifier, the user ID, the date and the time a violation was detected. There is also an indicator that shows the reason for logging. There are three indicators for authorization:

```
S       Access was granted due to SPECIAL attribute
O       Access was granted due to OPERATIONS attribute
A       Access was granted due to AUDITOR attribute
```

There are four indicators for audit options in SETROPTS:

```
C       Class audit was set
U       User audit was set
S       SPECIAL user audit was set
A       Access audit was set
```

A ″Y″ shows that the logging indicator was on; a ″N″ says logging was set to off.

4.3 QMF Hints and Tips

Most of the queries that are used to build the reports in the auditing application are simple SQL queries. However, to create reports you may need some means of decision making and passing of information from one query to another. It is for this function that QMF was chosen since it has a REXX interface that is used in building reports that require iterative queries and logic. As mentioned earlier, you need a least QMF Version 3 Release 1.1 since this is the first release with the REXX interface.

4.3.1 QMF Security Aspects

In most QMF installations, QMF is just another tool that is used by all those who have a need to use it. The QMF administrator has to define you as a valid QMF user and you can start working. To build reports, you have to be granted access to the DB2 tables that are built from the RACF SMF Data Unload Utility, meaning you need DB2 read authority as well.

If an installation wishes to further limit the extent of reporting that administrators or auditors are allowed to do, then DB2 views could be created granting them access only to what these views allow. Because of the nature of the contents of the DB2 databases built from the RACF SMF Data Unload Utility, you must protect them as you protect the SMF database itself. Make sure that the databases are not granted to public and also make sure that the SYSADM authority is limited to only a few people.

4.3.2 Modifying QMF Reports and Queries

The *auditing application base panel* has an option **Q - QMF -- Query Management Facility**, which takes you directly to QMF. Thus, if you have just produced a report that you would like to change, then you only need to return to the base panel, enter Q, and you are in QMF. It also means that the report you were just looking at is again shown, but now you can change the FORM, or the QUERY, or both, and produce a report that is more to your liking.

If you want to make your changes permanent, you have to save the FORM or the QUERY in the relevant members in QMF. Naturally, you have to have the necessary QMF and DB2 authorizations, but it is all fairly straight forward.

If you write your SAVE command in the format “SAVE FORM AS ?,” you will be prompted for the name, the confirmation option, the share option, and a possible comment. The prompt option should help to remind you to save your objects with the share option specified as “yes.”

If you are reporting on profiles with long names, you will find that these names come out truncated in the standard reports. We chose to do this in order to keep report line lengths to 80 characters where possible (no scrolling necessary).

If you find it necessary to display longer names, just change the QMF FORM specifications for the report in question, going back to the base panel and then into option Q.

The same thing holds true if for some reason you would like to change the sort order for a particular report. In this case, you would go into option Q, press PF6 to get the query that was last used, change the sort order, and run the query

again with your new sort order. Changes are temporary or saved permanently, depending or your needs.

Note that there is a naming convention for naming objects, in other words; procedures, queries, and forms in the package. All the names start with RCF, and the fourth character is P for a procedure, Q for a query, or F for a form. The last four characters are usually the same for a procedure that runs a query specifying a form.

However, some forms are used for multiple queries, so when changing a form for one query, you may be changing the form used by other reports as well. When in doubt, start by saving the original object under another name; then if you need it, you know where to find it. Always specify your objects as shared when you save them.

4.4 Modifying the Auditing Package

The auditing application as such is open-ended and lends itself to easy tailoring and growth. Basically, you may either change the existing objects as discussed in Section 4.3, “QMF Hints and Tips,” or you may create completely new selections by adding your new functions to the base panel or any of the sub panels or creating new panels. The easiest way to create new functions is to copy an existing function (choosing the one closest to what you need) and then modifying it to suit your needs.

The REXX EXECs that are invoked from the ISPF panels are all stored in the xxxxxxxx.RACF.EXEC data set and should be a good starting point for understanding the REXX callable interface in QMF.

4.5 ISPF Hints and Tips

ISPF panels are used by the auditing application to provide the interface between the user and the report application. These panels are modified to the way your installation uses ISPF panels.

Part of the user interface is the guidance provided by the help panels. The help panels are tailored to the way your installation uses the help function, and quite often it can be helpful to provide the user with the phone number of the help desk or a person to contact.

If you see a need for changing the information presented on the panels, you could always enter PANELID in your command field, after which you can obtain the name of the current panel. This then could lead you to the panel you want to change.

When translating the panel text to your own language, we would suggest you save the originals in a separate library for later reference, if need be.

4.5.1 ISPF Help Panel Structure

The help panels have been set up so that a user can either press the HELP key on the base panel and then be presented with all the options by just pressing the Enter key. Users can also select the particular option that they would like information about by the entering the number of the option they would like to view.

To make the changing of help panels easier, we have chosen to adopt a naming convention for the help panels as follows:

- All help panel names start with the characters RCFH.
- The next character tells us which panel the help text applies to, where B is for the base panel, U is for the user based reports panel, and G is for the group based reports panel.
- The last character or characters correspond to the option number on the respective panels.

The U and G panels have an extra selection with an option of zero. To explain how you fill in the selection fields at the top of the panel, let us try an example - you want to change the help text for the report “Profiles Owned by the User” (option 6 on the user based reports panel). The panel name is RCFH-U-6 if you follow the logic just explained.

You should be a little cautious when changing the panel attributes since, if you use the default attributes, you cannot use the percent sign in the panel text. Since you need the percent sign to signify a generic character in QMF, you have to define your attributes accordingly, at least for those panels that describe how user IDs, names, and the like should be entered. For more information, please read the note in Section 4.2, “Selecting Reports” on page 25. Other than that, you can change your help screens as you like using the attributes that are normal for your installation.

Chapter 5. The Workstation Auditing Application

Data processing security is mostly a question about policies, good common sense and verification that given rules are being followed. At many installations, security administration soon becomes too hard to handle with just one person, so you start doing distributed administration. Good security practice says that you should always try to maintain check and balance, so you also need distributed auditing.

It has been mentioned earlier in this book that the amounts of data involved in security auditing can be quite large. However, with distributed administration and auditing, the amounts of information for each individual auditor need not be larger than what could presumably be handled in a good size workstation. As an alternative, the audit databases could still be stored in a host computer, while the actual analysis could be performed on a workstation.

This chapter is trying to discuss some alternatives to auditing on the host computer based on DB2 and DB2/2.

5.1 OS/2 Environment

The following OS/2 programs were installed in the test environment:

Operating System/2	OS/2	Release 2.1
IBM DATABASE 2 OS/2	DB2/2	Release 2
Distributed Database Connection Services/2*	DDCS/2	Release 2.0
Visualizer Query for OS/2		Release 1.0
Visualizer Development for OS/2		Release 1.0

We assume that both OS/2 and DB2/2 are fairly well known, while DDCS/2 might be less well known. The DDCS/2 program provides a connection that expands the DB2/2 client/server environment to a client/server environment that can access host database management systems.

Clients supported by DB2/2, by using the DDCS/2 program, can define database objects and manipulate data in the DB2, SQL/DS and OS/400* database management systems. For more information on this product, see *Distributed Database Connection Services User's Guide* or *DDCS/2 Guide V2 with DB2/2*.

The Visualizer Query for OS/2 and Visualizer Development for OS/2 products are used as workstation query and presentation tools enabling users to produce applications for viewing tables and presenting the results in a fast and efficient manner. The Visualizer Development application includes an object-oriented language that is used to make prototypes of applications and production applications.

5.2 The Scope of a Group Auditor

The RACF Report Writer has long been accused of not being selective about what information the individual auditor has been allowed to report on. To tell you the truth, the problem is still there.

The only thing that you can rely on to be provided with each audit log record is the user ID. This means that if you have a clean RACF structure where all users

and resources are owned by groups, then it should be possible to build a table that says under which auditor′s authority a given user belongs.

Knowing this, you could also limit the information that a given auditor can see in terms of user information. However, it is not equally easy to draw the line when it comes to datasets and other resources.

Not all of the log records contain owner information, and you are now entering the zone where you would have to match information from the RACF database with the audit information. In other words, if I see an access to a resource, I would have to know which group owns the resource and then obtain who the auditor is, knowing the group name.

By combining the information in the tables that is built from the data produced by the RACF Database Unload Utility and the RACF SMF Data Unload Utility, you can obtain the likely auditor for each log record, but it takes more than a simple view or a simple SELECT statement to find the information.

Audit record selection based purely on user ID will probably give some conflicting results. As a group auditor, you are certainly interested in finding out what your users are doing in terms of access violations and the like. However, if there had been an access violation on say ″SYS1.LINKLIB″, the owner of that dataset is definitely interested in knowing this too. The question then is who should really be the recipient of the access violation message, the owner of the resource or the owner of the user who did it? The answer is probably that both parties should see the violation, and this then makes record selection based purely on user ID impossible.

The aim of the above discussion is to show the need for a clean, clear-cut policy for profile ownership and database structure for the RACF environment. If your structure is clean, you should be able to build additional tables with the information provided by the utility programs mentioned before. However, you should not plan building these scope-of-group tables dynamically for each request, but rather when you have loaded your RACF database tables with new information.

Having created scope-of-group tables for your auditors, you would then be in a position where you can filter from all the other data the data that a specific auditor is allowed to see. Again, it is not simple but you will probably have to do it in an environment where distributed administration and auditing is being used.

With a your scope-of-group table prepared, it is probably feasible to download SMF information for a group auditor to a PC. The total amount of data produced at a good size installation is probably too much for a PC. By downloading data onto the PC, you would only have to make the filtering in connection with the download.

If you only want to use the tables that are stored on your host system to do reporting, you will have to create views or construct some other kind of filter to be used for every query made by the auditors from their workstations.

This chapter describes an workstation auditing application that is based on the Visualizer Query for the OS/2 product. The main parts of the workstation auditing application are shown in Figure 25.

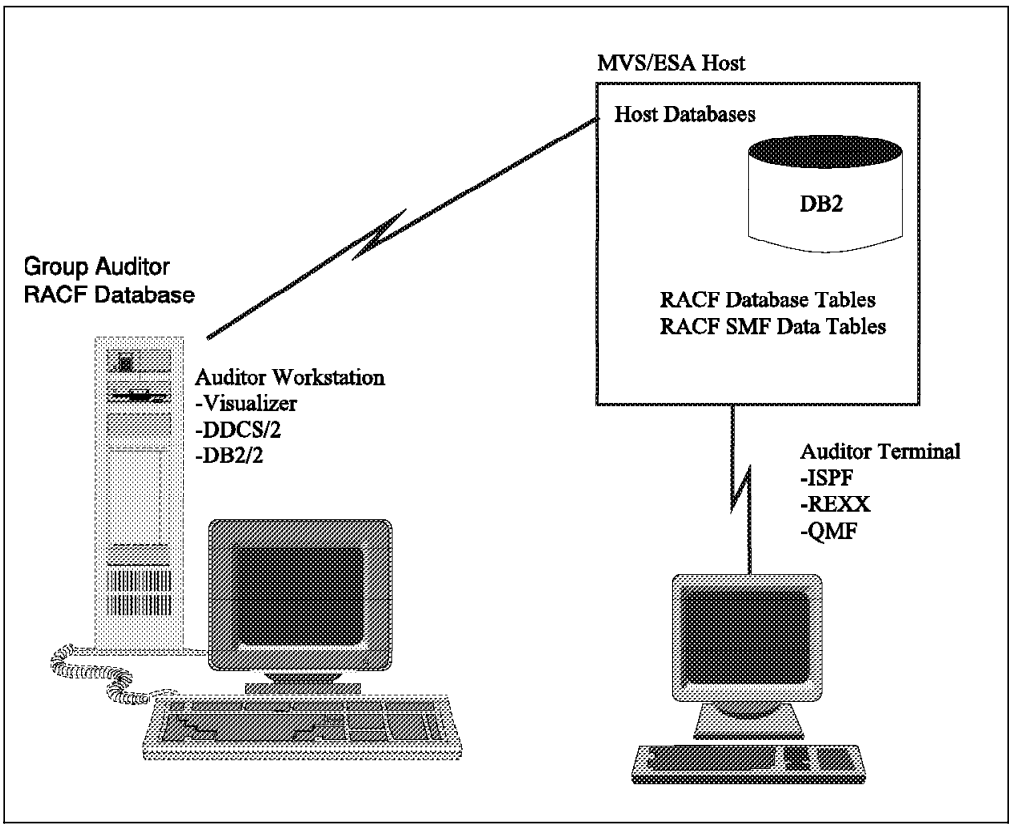


Figure 25. Workstation Auditing Application Overview

5.2.1 Installing the Workstation Auditing Application

To install the Visualizer Query for OS/2, refer to the documentation that is shipped with the product.

To install the workstation auditing application, you only need to copy the file containing the application to a suitable OS/2 folder. In so doing you will now have an icon created onto you desktop from which to start the application.

Note: For information on how you may obtain a copy of the application that is discussed in this chapter, see 1.1, “How to Order Materials Discussed in This Document” on page 2.

The choice of location for the databases to be used for reporting is up to the installation. The application does not have to be changed depending on the placement of the databases; it just requires changing a few parameter values, and you need a process to load the tables onto the workstation. The decision to be made, therefore, is one of available storage space in the workstation and what level of protection you can provide for the information on the workstation.

Be advised that to run the auditing application using host based DB2 tables, you need the proper authorizations. Your user ID will, therefore, have to be a RACF defined user ID with the necessary DB2 authorizations.

5.2.2 Using the Workstation Auditing Application

When you start the workstation auditing application, a window like the one shown in Figure 26 is created.

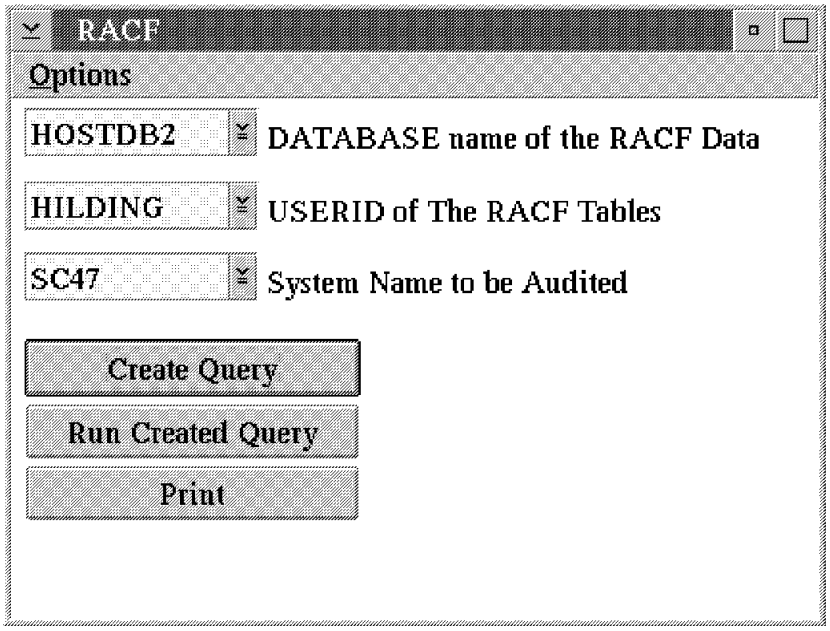


Figure 26. Workstation Auditing Application Main Panel

The database names shown and the user ID of the table owner are initialized for you by the *Visualizer* application. You can use the drop list to the right to choose one of the available names. The name of the system to be audited is the SMF ID of the MVS/ESA* system that produced the log records. Again the Visualizer application will find the available values for you.

Having made your choices, you should select the **Create Query** button. This will result in a window similar to the one shown in Figure 27.

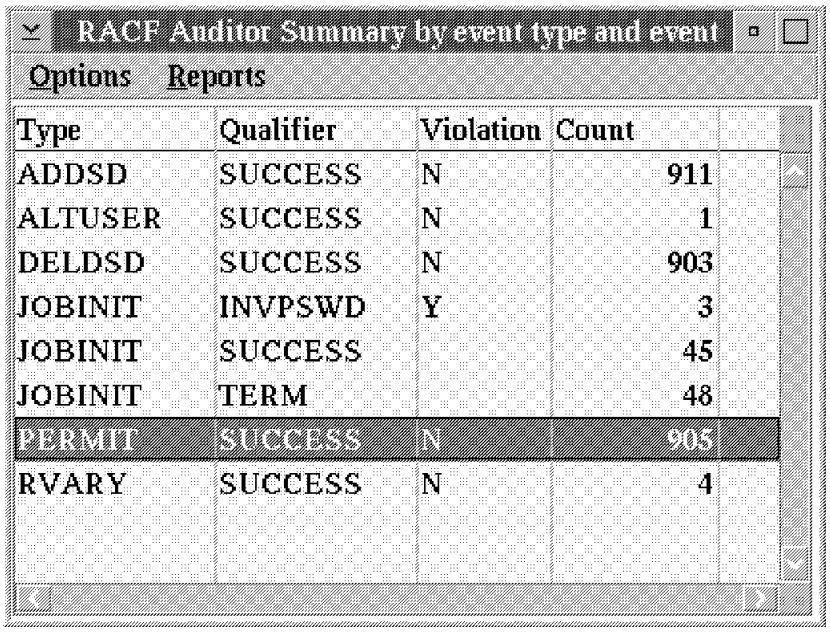


Figure 27. Sample Visualizer Summary Report

The window shows a summary of all events that have taken place based on the selected DB2 table information. To create a report, you only need to select the event type that you are interested in and select the **Create Query** button from the main window. This will result in yet another window with all the field names defined in the DB2 table for this event type.

Figure 28 shows the a partial list of field names in the record logged when you do the RACF PERMIT command.

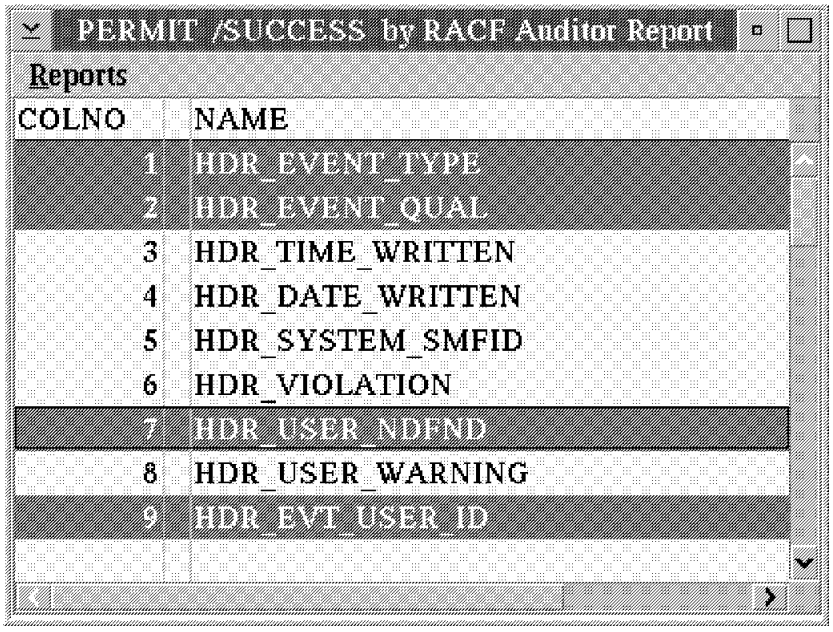


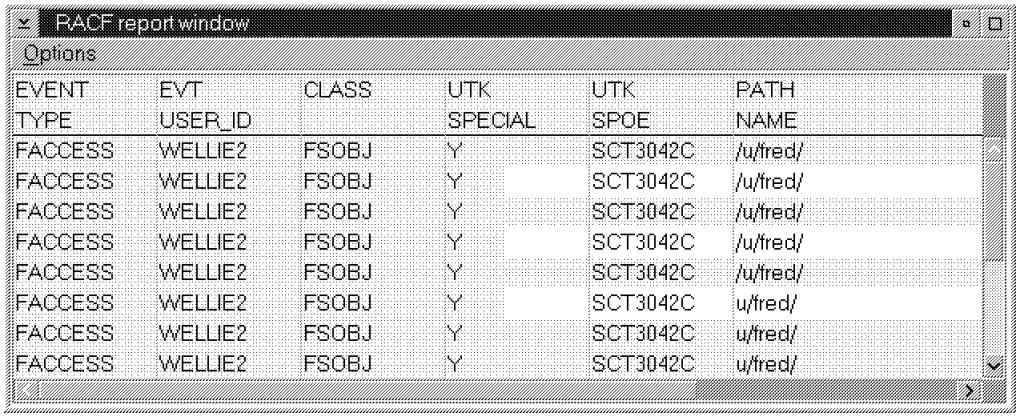
Figure 28. Field Names in the DB2 Table for a Specific Event

From the list of fields names, you may now select the ones you want to see in your report. A few of the fields are already selected by default (as shown by the highlighting) and are deselected by selecting them again. When you are

satisfied with your selections, you should select the **Run Created Query** button from the main panel, and your report will be created.

Remember that as long as you want to be able to view the report on your workstation, you should not be selecting too many fields at once, since this results in your having to scroll left and right all the time. Soon enough you will determine which fields contain the important data as opposed to data that occurs many times in different shapes.

Figure 29 shows a report on the check file access events (FACCESS) which are produced when you run OpenEdition* MVS.


RACF report window

Options

EVENT TYPE	EVT USER_ID	CLASS	UTK SPECIAL	UTK SPOE	PATH NAME
FACCESS	WELLIE2	FSOBJ	Y	SCT3042C	/u/fred/
FACCESS	WELLIE2	FSOBJ	Y	SCT3042C	/u/fred/
FACCESS	WELLIE2	FSOBJ	Y	SCT3042C	/u/fred/
FACCESS	WELLIE2	FSOBJ	Y	SCT3042C	/u/fred/
FACCESS	WELLIE2	FSOBJ	Y	SCT3042C	/u/fred/
FACCESS	WELLIE2	FSOBJ	Y	SCT3042C	u/fred/
FACCESS	WELLIE2	FSOBJ	Y	SCT3042C	u/fred/
FACCESS	WELLIE2	FSOBJ	Y	SCT3042C	u/fred/

Figure 29. Sample Report for Check File Access in OpenEdition MVS

5.2.3 Visualizer Query for OS/2 and Visualizer Development for OS/2

Figure 30 shows the process of building your own *Visualizer Query* application. What you do is define your menu consisting of a menu bar entry and a list of menu choices. You then define one or more windows, which are areas with a border used for conducting a dialog with the user or presenting a view of an object.

The *Visualizer Development for OS/2* will then analyze your menu and your window contents and produce skeleton code that corresponds to your definitions. An application developer can now take the skeleton code and fill in the actions that are to take place because of a certain selection and so forth.

When the programmer is done filling in the code for the various actions, selections and options, the code is sent to the special compiler to be built into an application for you.

The Visualizer Development for OS/2 is only needed by those who write applications. The *Visualizer Query for OS/2* is needed if your applications use functions like SQL queries.

The above introduction to the Visualizer product is only there to give you a feeling for what the products do. In developing the sample auditing application for the OS/2 workstation, the Visualizer products made the development quite easy, and this would show that whatever additional tailoring needs to be done should also be fast and easy.

The sample application for the OS/2 environment also gives the auditor some facilities that are not available in the ISPF application, such as being able to dynamically select the information you would like to report on.

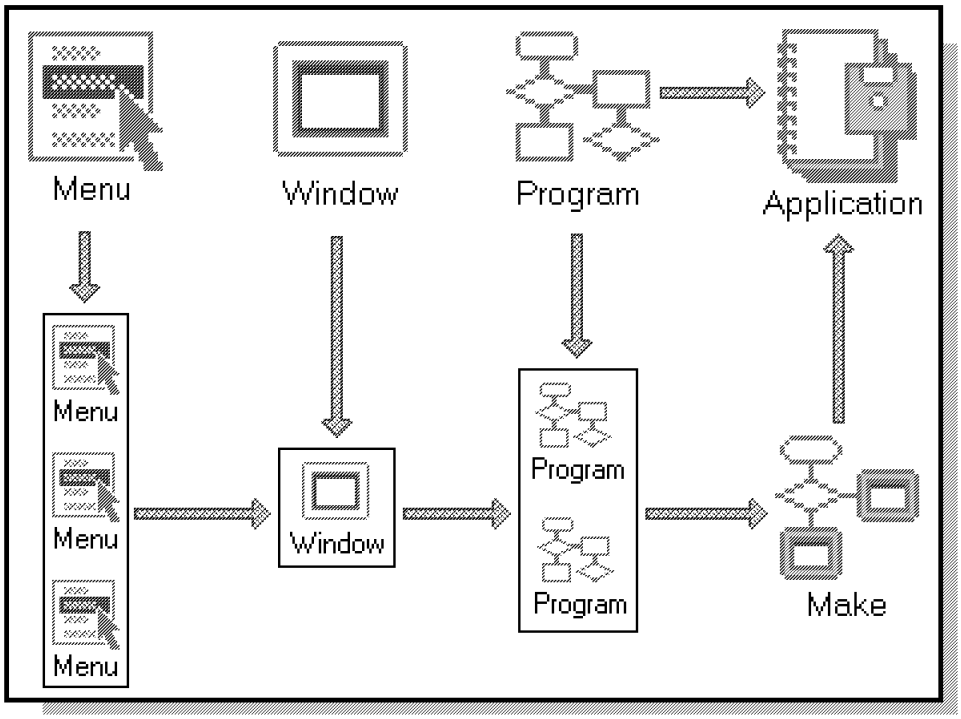


Figure 30. Overview of the Visualizer Application

5.3 Producing Reports Using DB2/2 and SQL

If the Visualizer Query for OS/2 or equivalent product is not installed on your workstation, you could use a simple REXX procedure as a starting point for producing auditing reports. The following sections describe such a sample REXX procedure and how it works.

The REXX procedure does SQL queries to produce predefined auditing reports. If you are familiar with REXX and SQL, it should be fairly easy to add additional queries to the REXX procedure and to tailor the reports to suit your needs.

The REXX procedure presupposes that you have the DB2/2 and the DDCS/2 products installed in your workstation and that your DB2 tables are loaded in your MVS host. This being the case, you will have to establish contact with the host by going into the *DB2/2 Command Line Processor*. You establish contact by issuing the command:

```
DBM START USING DATABASE database_name
```

If you have not already signed on, you will be prompted to do so now.

Still from your DB2/2 Command Line Processor window you can now start your auditing procedure by entering **audit**. The REXX procedure main selection panel

will now be shown as in Figure 31, and you can select what kind of report you would like to see.

The main panel has the following select options:

- Reports about resource accesses
- Reports about accesses by a specific user
- Reports about RACF command utilization

```
          AUDIT REPORTS


      1   Specifying DATE AND TIME

      2   Access to a specific resource

      3   Using RACF commands

      4   Events by a specific user

      9   EXIT
```

Figure 31. REXX Procedure Main Selection Panel

As described in Chapter 4, “Using the Auditing Application and Sample Reports” on page 25, you can limit the amount of data by specifying date and time. This is done by selecting option **1** from the REXX procedures main selection panel.

5.3.1 Reports on Resource Accesses

Resource access reports are selected by option **2**, and results in additional panels where you specify whether you want the report based on resource name or if you want to see a report showing all successful accesses, all failed accesses or accesses granted because of warning mode.

The resource name specified when you want to look at specific resources can either be fully qualified or partial by using the generic character (a percent sign).

Figure 32 shows a sample report on resource accesses.

```
ACC_RES_NAME   ACC_CLASS   ACC_NAME   ACC_OWN_ID  ACC_VIOLATION  USER_ID
------------   ---------   --------   ----------   ------------  -------

SYS1.MANY      DATASET    SYS1.MAN%    OWNER1          N          USER1
SYS1.MANY      DATASET    SYS1.MAN%    OWNER1          N          USER2
SYS1.MANY      DATASET    SYS1.MAN%    OWNER1          Y          USER3
SYS1.MANY      DATASET    SYS1.MAN%    OWNER1          N          USER4

  4 record(s) selected.
```

Figure 32. Sample Report on Resource Accesses

5.3.2 Reports on Events Caused by a Specific User

Option **4** on the REXX procedure main selection panel will produce a report on the events that a specific user has caused to be logged. First you will see another panel where you can specify that you want a report on all users, a specific user only, or a report on violations only. When specifying a specific user name, you can again use the generic character (the percent sign) to report on all users who satisfy that generic name.

A sample report on events caused by a specific user is shown in Figure 33.

```
HDR_EVT_USER_ID  HDR_EVENT_TYPE  HDR_TIME_WRITTEN  HDR_DATE_WRITTEN
---------------  --------------  ----------------  ----------------

USER01           ACCESS          18.17.23          1994-08-16
USER01           ACCESS          18.17.23          1994-08-16
USER01           ACCESS          18.17.25          1994-08-16
USER01           DEFINE          18.17.26          1994-08-16
USER01           ACCESS          18.17.28          1994-08-16

  7 record(s) selected.
```

Figure 33. Sample Report for a Specific User

5.3.3 RACF Commands Report

You can produce a report showing the use of some important RACF commands by selecting option **3** on the REXX procedure main selection panel. On the next panel, you can select one of the following commands: ALTGROUP, ALTUSER, CONNECT, PASSWORD, PERMIT and RALTER.

Figure 34 shows a RACF commands report.

```
PERM_EVENT_TYPE  USER_ID  TIME_WRITTEN  DATE_WRITTEN  PERM_RES_NAME
---------------  -------  ------------  ------------  --------------

PERMIT           USER1    18.23.08      1994-08-16    USR.BASIS.TEX
PERMIT           USER2    18.23.09      1994-08-16    USR.BASIS.TAB
PERMIT           USER1    18.23.11      1994-08-16    USR.BASIS.TEX
PERMIT           USER3    18.23.23      1994-08-16    USR.BASIS.TAB
PERMIT           USER5    18.23.34      1994-08-16    USR.BASIS.TEX
```

Figure 34. Sample RACF Command Report

Chapter 6. The Enhanced Reporting Application

This chapter describes the various reports that you can obtain with the enhanced reporting application. These reports are selected via selections **1** through **12** on the auditing application base panel as shown in Figure 12 on page 20.

6.1 Selecting Reports

The auditing application base panel has the following major sections:

- User based reports
- Group based reports
- Profile based reports
- Summary reports
- Access list clean-up

Selecting reports other than the summary reports is normally a two-stage operation in which you first build a list of candidates, and then select one or more entries for which you want details. Remember that since QMF is used as a query manager, the percent sign (%) is used as a generic character and not the asterisk (*), which is otherwise the case.

Note: Keep in mind that specifying U1 for a user name or user ID is interpreted by the package as U1%, meaning all the user IDs or user names starting with the characters U1. You can also precede a character string with the percent sign, meaning you can search for a name such as %ANNE% in the user name field.

6.1.1 User-based Reports

User-based reports are selected from your base panel by selecting option **1 - User based reports**. This option takes you to the panel that you see in Figure 35. You start by selecting the user IDs that you are interested in by entering either a fully qualified user ID in the user ID field or by entering a partial user ID preceded or followed by a percent sign, or enclosed by percent signs, depending on what you are looking for.

You can also do your lookup by entering a user name or partial name as it appears in the user name field in the RACF profile. Having entered your selection, press Enter and see either the single entry you requested or a selection list from which you pick the entry of your choice by entering any character before the user ID.

Your chosen user ID now appears on your selection panel; only now there is a user ID and the name of that user as entered in the user name field. You can now choose to see the various reports about this user, starting with the groups the user is connected to and ending with RACF profiles that are within the scope of your selected user.

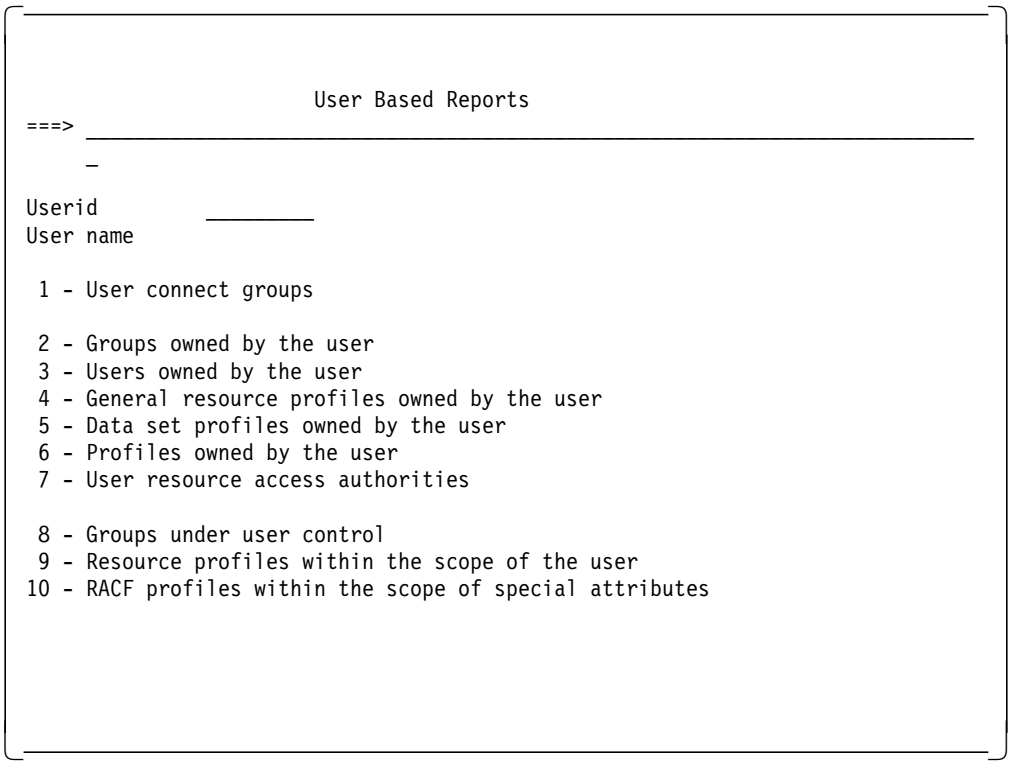


Figure 35. RACFUS01 User Based Reports Panel

Depending on your choice of output (QMF or BROWSE), there is also a difference on what you can do with your reports. BROWSE lets you use FIND commands and scrolling up, down, and sideways; while QMF output allows scrolling but not the use of the FIND command. If you want to print the reports you have produced, QMF output lets you do that.

The following reports may be produced:

User Connect Groups: Gives you the names of the groups to which the user is connected. Normally, the groups represent the different duties of the person and are used to give that person access to resources necessary to perform these duties.

An auditor or administrator would use this report to verify that a user is not connected to groups that represent duties that a person no longer has or is not supposed to have.

Groups Owned by the User: Some installations use group ownership as a means of distributing administrative duties. This report shows what groups the user owns and hence the groups that are under this user's control.

The report could be used to obtain which part of the group structure is under a particular user's control and if this is in line with the installation policy.

Users Owned by the User: A person who is a local administrator for a department or group can perform his duties either by being the owner of the users in that department or group or by having the group-SPECIAL attribute. This report gives a listing of all users that are owned by a particular user ID.

The report would be used to verify that users owned by another user are all part of the same department or group and that there are no old user IDs left that could be misused by the owner.

General Resource Profiles Owned by the User: All resource profiles that are not data set profiles are considered general resource profiles. This report shows all the nondata set profiles that your chosen user owns.

Use the report to verify that administrators have not forgotten to specify correct ownership when defining resources. When you define a resource profile, the RACF default is to make you the owner of the profile and to put you on the access list with ALTER authority for all profiles that are not based on your user ID. In order not to have administrators on all access lists and as owners for all the resources they have defined, installations often build their own RACF panels or REXX EXECs to remove the access list entries and to enforce group ownership instead of the normal default.

Dataset Profiles Owned by the User: Normally, a user should own only those data sets for which he carries the full legal responsibility. In most installations, resources tend to be owned by groups that represent a given task or responsibility. However, a user should at least own the data set profiles for his personal data sets (userid.** and so on).

The report is used to verify that a user owns only those data set profiles that he is supposed to own. Frequently, this report shows administrators as owners of those data sets for which they have defined the profiles, simply because the ADDSD command makes the issuer the default owner. Use this report to identify errors where administrators have forgotten to specify the correct ownership for resources that they define.

Profiles Owned by the User: This report lists all the profiles that your chosen user owns. The report is not limited to resources but includes users and groups. For a normal RACF user, this is probably the fastest way of finding out what the user owns. For local administrators, where they have not monitored profile ownership, the report might be quite large, and you may elect to print it out.

Individual ownership is not the normal or preferred way of handling RACF profile ownership. Use this report to check that individuals have not been defined as the owners of resource profiles or users and groups. Where such ownership is present, use the report as the basis for changing the ownership to the proper group in your RACF structure.

User Resource Access Authorities: The report shows those resource profiles that a given user ID can access, either because the user ID is on the access list or because one or more of the user′s connect groups are on the access list. The report also shows all resource profiles that the user is allowed to access because the profiles either have a universal access that is not NONE or because the ID(*) (all RACF defined users) is on the access list. The report shows the resource class, the resource name, the access allowed, the reason for allowing access (user ID, group name, UACC, or *) and which DB2 table was used as the source of information. Profile names have been truncated to 30 characters to avoid scrolling left and right for terminal output. If your profile names are often more than 30 characters long, you just have to change the QMF form specification to see the full name.

What are my resource access authorities is a frequently-asked question at most installations. If you use the “list-of-groups” access checking, this report shows you what resource profiles you are authorized to use. However, that does not automatically translate into what actual data sets you are allowed to use, since you have to match profiles against catalog information.

This kind of profile matching does, however, require an understanding of the logic that RACF uses when matching profiles, and also requires the reporting tool to be run on the host where the database unload was done. When the tool was designed, the requirement for the tool was that it never have to run on the same host as the RACF database itself.

There are some points that auditors might want to remember when looking at the user′s resource access authorities, as detailed in this report. The first thing to note is the number of entries to which a universal access authority higher than READ applies. These should be few. The data sets and other resources where a universal access of READ applies should not include personal data sets or group data sets other than system data sets where there is a common need for the universal access. Often, the universal access would be better served by allowing the access through the Global Access Table instead. The ID(*) on an access list at an installation where you have specified SETROPTS JES(BATCHALLRACF) is for all practical purposes equal to universal access for that same resource. Again, you should not allow ID(*) to be used extensively by resource owners because it normally means that they have not built a valid access list.

Groups under User Control: When administering RACF in a decentralized environment, the group administrators are usually given the group-SPECIAL attribute. This means that the administrators can exercise their special rights only within the scope of their group or groups. When building a report of the groups that are under a given user′s control, the groups that are included are those where the user is defined as having the group-SPECIAL attribute and the subgroups owned by this group or its subgroups. We chose not to do this for users that are SPECIAL on a system-wide basis, since these users have a scope that is the total system.

The report shows the group name, the owner of the group, the group′s superior group, and the group level. A level of zero implies the highest level, and one is added one for each next lower level. Compared to a limited groups report as produced by DSMON, this report does not show those groups in the structure that are not within the scope of the user.

Use this report as a system administrator or system auditor to verify that a local administrator can administer only the structure of groups that he is supposed to. If you find groups within the scope that are not supposed to be there, it means either that the user has been given the group-SPECIAL attribute in the wrong groups or that another group-SPECIAL user has made a CONNECT that is not supposed to be there.

Resource Profiles Within the Scope of the User: This report shows those resource profiles where the user is either on the access list as an individual user or as a member in a group. The information presented is the profile name, resource class, access allowed, access ID, and a reason. Some profiles may be owned by the user, and for these profiles, the reason field is set to SCOPE and the allowed access to ALTER.

RACF Profiles Within the Scope of the User: The scope of a user is defined in this report to mean the RACF profiles owned by the user (for a normal user) or the RACF profiles owned by the user plus the profiles within the scope of the group where the user has the group-SPECIAL attribute. In addition to resource profiles, you will also see profiles for users and groups if the user owns any. A good security policy should state clearly that resource profiles should always be group owned. Use this report to verify that the rules are adhered to and that the group-SPECIAL users do not have a scope that is larger than expected.

6.1.2 Group-based Reports

Group-based reports are selected from your base panel by selecting option 2. Option 2 takes you to the panel shown in Figure 36. Start by selecting the group name that you are interested in by entering either a fully qualified group name in the group field or by entering a partial group name preceded or followed by a percent sign or enclosed by percent signs, depending on what you are looking for. You can also do your lookup by entering all or parts of the information appearing in the installation data field in the group profile, again using percent signs to signify a generic search. Having entered your selection, press Enter to see either the single entry you requested or a selection list from which you pick the entry of your choice by entering any character before the group name.

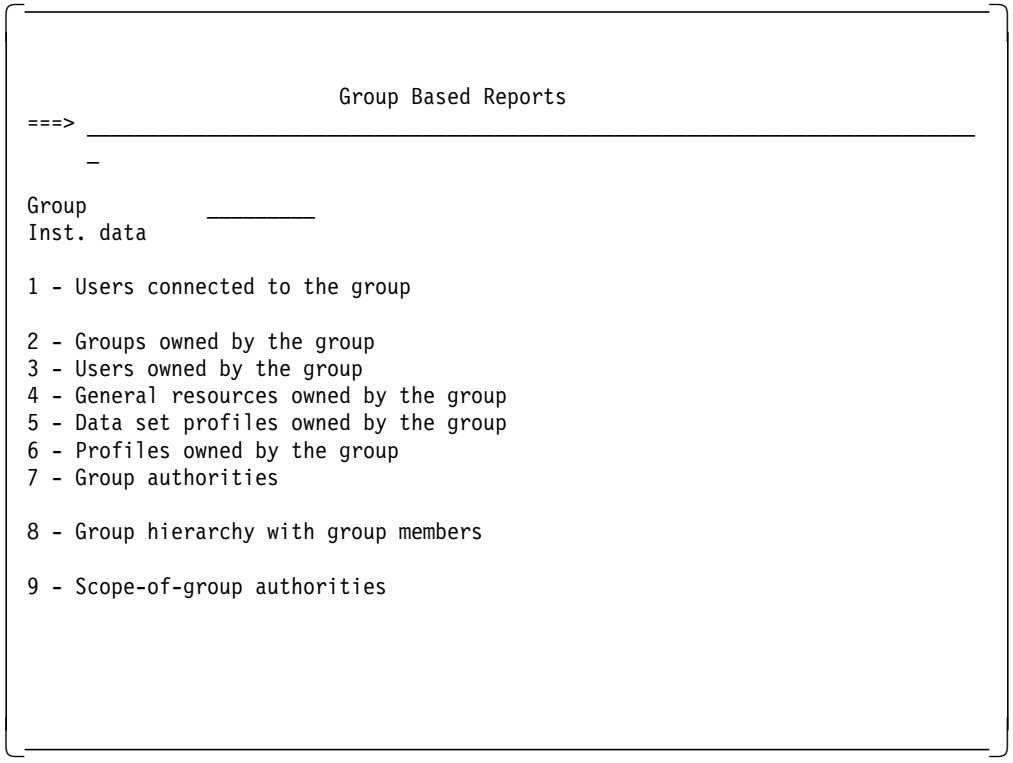


Figure 36. RACFRY01 Group Based Reports Panel

Your chosen group will now show up on the panel from which you started, only now there is the group name and the information from the installation data field, where used. You can now chose to see the various reports about this group, starting with the users connected to the group and ending with the scope-of-group authorities.

Depending on your choice of output (QMF or BROWSE), there is also a difference as to what you can do with your reports. BROWSE lets you use FIND commands

and scrolling up, down, and sideways; while QMF output allows you to scroll your reports and print them but, does not let you use the FIND command.

The following group-based reports are available:

Users Connected to the Group: The report shows which users are connected to the group you have chosen. Both user ID and the user name are shown on the report.

Reports showing which users are connected to a group are used in several ways. Assuming you have a RACF database structure where you use resource protection groups, functional groups, and administrative groups, you can use the report to verify that there are no users connected to resource protection groups. You could also obtain a report showing all the users in a department or group and get it signed by the department manger or group leader. For functional groups, you could also verify that users of that group are in fact still engaged in the task that it represents.

Groups Owned by the Group: The report shows the groups that are owned by your selected group, the date that the groups were created, and installation data where present. The report shows only the groups that are directly owned by the group, not the full scope of the group.

When you want to know what groups would have to change ownership when deleting a group or moving it in a structure, this report is helpful. Since it shows only the groups directly owned by the group, you know what groups are directly affected by a change.

Users Owned by the Group: Security is a matter of having a clear policy, good naming standards, and a structure to make security administration not only possible, but easy. The output of a report showing what users are owned by a particular group is, therefore, meaningful only if you have a structured ownership of user profiles.

If you have a policy where all users are owned by the administrative group that represents their department, this report would show you all user IDs and the names of those individuals that work in the department. You will also have information about when the user profiles were defined and when a user ID was last used. All this information is used to verify that the right individuals are owned by a group, and could also be used to match the information against the personnel file or to make it possible to distribute information about security violations to the proper department.

General Resources Owned by the Group: Profile ownership is an important part of setting up a RACF security structure. Since users tend to change jobs and change departments, profile ownership should not be based on users. Instead, you define groups that are the logical owners of resources representing a department, a job function, or task on behalf of which this resource is defined.

Let us assume you have a CICS* system with many applications, and you want to control the transactions belonging to each application. To make controls more manageable, you would define groups that represent each application. When defining the groups, you should try to describe what the groups represent by using the installation data field. You would then define your CICS transactions and make the group representing the application to which the transaction belongs the owner of the profile. Reports about the general resource

profiles that are owned by a given group in this kind of an environment is used by administrators and auditors to verify that the resources reported on are the right ones. The report shows the class name, the universal access for the resource, and the resource name.

Remember that what you see in this report are the profile names that are owned by the group. Since you may be using generic profiles, there could be additional resources protected by the profiles listed.

Data Set Profiles Owned by the Group: The first-level qualifier of a data set should, where possible, represent the owner of the data set. There are, however, several data sets that are part of the operating system, program products, or some general applications where the first-level qualifier is fixed and where an owner is not obvious.

This report shows you the data set profiles that are owned by a given group, giving you the data set name and the UACC that applies to the data set. Once again, you should remember that this is not a list of the data sets that are owned by the group but only the profiles used to protect those data sets. If you would like to know the actual data sets that are protected by these profiles, you would either have to run a series of LISTDSD commands with the DSNS operand or make a query to match these profile names against a catalog listing.

Use this report to verify the existence of relevant profiles and to verify that the UACC specified is relevant to the data sets it is protecting.

Profiles Owned by the Group: This report shows not only the general resource profiles and the data set profiles that the group owns, but also users and groups that the group may own. The report is a fast and easy way of verifying that an administrative group owns only users and no other resources. In other words, you use this report to see that your ownership rules are being followed and that you do not mix administrative groups with functional groups or resource-protection groups.

Group Authorities: The group authorities report lists all those RACF profiles with the group on the access list. The group represents a task or a job, and what the report shows is what resource profiles a user performing this task can access. The report lists the resource class for each profile along with the profile name, the access authority, and the DB2 table name from which the information has been extracted.

This report is useful for verifying what resource profiles a given job or task can access. As an auditor, you would also try to assess whether the access authority reflects the needs of the job and the intentions of the profile owner. You could also use the group authority report to serve as a model to define new groups to reflect similar tasks.

Group Hierarchy with Group Members: Option 2 provides a report called “Groups owned by the group,” that shows you the groups owned by the selected group. In this report you add the users connected to each of the groups in this structure. For every user ID, you also have the programmer name, last access date, and the special attributes given to this user ID. The special attributes are listed both on a system-wide basis and on a group-connection basis.

Administrators and auditors should find this report useful for quickly answering questions about the users that are connected to a group structure. They can

also find out what attributes these users have been assigned. The last access date is useful when trying to find user IDs that are not being used. Usually, these user IDs should be revoked, but where a user ID has been defined and never used, it will not be automatically revoked. Such user IDs can often pose a danger in that they may have a default password (equal to their default group), or the password might be a value known to most employees (always assigned to new users).

The user attribute columns may need a separate explanation. To fit the information in as small a space as possible, we chose to format the listing so that the S-REV, S-SPEC, S-OPER, and S-AUDIT headings and their group level counterparts G-REV, G-SPEC, and so forth are written vertically. An S-REV value of "Y" means the user is REVOKED on a system-wide basis and cannot sign on to the system or submit a job. A G-REV value of "Y" means that the user is revoked from this group and is not able to sign on with this group as the current connect group or to use the authorities within this group. S-SPEC stands for the system-wide SPECIAL attribute; OPER stands for the OPERATIONS attribute; and AUDIT stands for the AUDITOR attribute.

Scope-of-group Authorities: The heading for this report reads "RESOURCE PROFILES OWNED BY xxxxxxxx OR ITS SUBGROUPS" and is perhaps a better explanation as to what the report shows. What you see is a listing of resource profiles giving the resource class, the name of the profile, the universal access (which is set to ALTER), and the owner of the resource profile. The universal access is set to ALTER since the owner of a resource profile can always change it. As an administrator with the group-SPECIAL attribute, these are the resources that you can manipulate under the group structure you are just viewing. Note that in addition to the resource profiles directly owned by the group or its subgroups, you will also get the resources that are owned by the users that are owned by the group structure.

The value of a report like this depends on the group structure you are looking at. If your policy does not clearly state how resources should be owned and by whom, then you will see random resource profiles being owned in the group structure. If you have made a decision to have groups for resource ownership and specific administrative groups (departments) and functional groups (jobs or tasks), then you are likely to find the information in this report much more useful. You can see all the resources a group administrator can handle and which group in the structure owns the various resources. If what you see does not adhere to your naming standards, or you see resources that do not belong there, then the profiles should be revised accordingly.

6.1.3 Profile-based Reports

There are two reports that are based on finding specific information in resource profiles. The first report type (option 3 on your base panel) is based on locating all profiles with a given value for universal access. Option 4 on your base panel provides you with ownership and access list information for the profile you select.

Profiles Based on UACC: Having selected option 3 on your base panel, you will be transferred to panel RACFVA01 where you need to fill in only the value for the universal access of the profiles you wish to see. The resulting report shows you the resource class name, the universal access, the owner, and the resource name of all the resources that have the selected value for the universal access.

Use this report as a quick check for detecting misuse of the universal access specification. Since universal access applies to all users (even those not defined to RACF), you should always specify a universal access of NONE for resources that have a real need for protection, either because they are needed for availability reasons or because they contain classified information.

Profile Information: The profile information report (option 4 on your base panel) takes you to panel RACFPF01. From this panel you can select the profile name and the class name of the profile you wish to see, or you can do generic selections for both profile names and class names. Specifying “V” on the command line provides a selection list; specifying “1” provides the profiles matching your selection.

Say that you select SYS1 as the profile name and DATASET as the class name, enter V (or leave blank) for a selection list, and press Enter. A selection list of all profiles starting with SYS1 will be produced. Enter any character in the “Sel” field for the profile you want, and a report is produced for that profile. If you enter exactly the same information for profile name and class name as in the previous example, but enter a “1” instead for profile report, you will obtain reports for all data set profiles that start with SYS1.

The selection lists that are the result of your entering a V or leaving the command field blank contain information about the resource class, profile name, universal access, and profile owner. Profile reports contain all the information from the selection list and access list information, including the authorization ID, access allowed, programmer name or group installation data (where applicable), and a message indicating whether the authorization ID is a group or a user. You may also see a message saying “UNKNOWN USER OR UNKNOWN GROUP,” indicating that the identity on the access list no longer exists in the RACF data base.

Profile reports are handy where you do not remember the class or the name of a resource you are looking for. By specifying the class and the profile name generically, you get a selection list from which you can find what you were looking for.

6.1.4 Summary Reports

Summary reports are the last six report options on your base panel, and they all produce reports without any additional input. Some of the reports are called *compressed reports* since they show as much relevant information about each resource profile as can be fitted on a single line. Let us have a look at each of the summary reports.

Compressed General Resource Report: The compressed general resource report gives a fast overview of all the general resource profiles that are defined on the system from which the database-unload was made. The information displayed includes resource class, resource name, profile owner, the universal access allowed, whether if warning mode is specified for the profile, and what security level the profile has. Remember that the security level is shown here as a numeric value, but is really a translation of whatever has been specified in a RDEFINE command for SECDATA SECLEVEL.

The obvious fast check to make based on this report is to see that the universal access specified is within the expected range and that warning mode has not been left on for profiles that should really work in fail mode. You should also

check to see that profile ownership is by group and not user ID (providing this is what your policy says).

Compressed User Profile Report: This report is designed to take just a few important fields from every user profile and to show them on a single line. The information includes the user ID, programmer name, default group, date and time of last access. When in BROWSE, mode you can use the report as an easy way to find the programmer name for a given user ID or to find the user ID for a given programmer name.

From an auditing point of view, the report gives you information about the last time a user logged on to the system, which can sometimes be helpful in determining whether a user ID is active. For user IDs that have never logged on to the system, the last access date and time are shown as "-," and this kind of a user ID is one potential starting point for a system attack. Most hackers and system programmers know that the initial password for a newly defined user is equal to the name of the user′s default group, unless the person that does the define explicitly changes that. Some installations always use a fixed password as the initial password, which is yet another risk for attack.

Compressed Group Profile Report: The compressed group profile report shows all the groups that were defined in the RACF data base when the database-unload was made. The groups are shown in alphabetical order, and the information consists of group name, group owner, the group′s superior group, and subgroup or subgroups if there are any. The group report is probably easiest to view in BROWSE mode since it is fairly extensive in large installations, and you most probably want to be able to use FIND commands.

The compressed group profile report is used for many purposes, such as to obtain what subgroups there are, where a group belongs in the group structure, who owns the group, and whether it is user or group owned. If you use a naming convention for your groups, you may also be able to understand the structure of neighboring groups. It is a fast way of locating groups and understanding their place in the group structure when you are planning changing that structure, deleting groups, adding groups or changing ownership.

Compressed Data Set Profile Report: Depending on the number of data sets at your installation and the number of profiles defined for each high level qualifier, this could be a very large report. BROWSE mode is recommended for viewing at the terminal since you are most likely to want to use the FIND command. The report shows you the data set name, the owner of the profile, the universal access, whether warning mode is in effect for the profile, and the security level assigned. The security level shows the numeric equivalent of the security level as explained under the compressed general resource profile report.

The points of interest in this report include the obvious loopholes, such as UACC of UPDATE or higher, warning mode in effect for the profile, and no security level specified where your policy demands otherwise. These examples are but a few of the uses for the report. The BROWSE command can help you find information in the report. Say that you want to locate all profiles that have warning mode specified. You start by entering COLS on the command line, which gives you a ruler at the top of your screen. By looking at the ruler you can determine that the warning mode indicator is in, say, column 69. You then enter **FIND Y 69**, and BROWSE will find the first occurrence of the warning mode indicator with a value of Y. To repeat the search for the next occurrence, you would normally just have to press PF5 (repeat FIND). The same principle applies for finding a UACC with

a given value, or anything that you want to locate in a fixed column of your report.

Since the compressed reports are fairly large, you should make certain that the data set used to hold them is large enough. If you get an X37 ABEND because of a larger than usual report, you can split the screen and make a reallocation under ISPF without having to leave the reporting tool.

Users and Their Connect Groups: This report is a bit different from the other summary reports in that you have a multiline output format for every user. A sample report is shown in Figure 37 to make it a bit easier to understand the structure of the output.

```
USERS AND THEIR CONNECT GROUPS

USERID   PROGRAMMER NAME        CREATED     LAST ACCESS         R A S O
                                            DATE       TIME     E U P P
                                                       .        V D C R

SPREEN   TEST                    1993-04-21 1993-02-05 18.20.23  Y N N N

  GROUPID   REVOKE   AUDIT    SPECIAL  OPER
  --------  -------  -------  -------  -------
  TEST      N        N        N        N



SRCDAWS  GEORGE DAWSON          1993-05-07 1993-05-14 15.59.25  N Y Y Y

  GROUPID   REVOKE   AUDIT    SPECIAL  OPER
  --------  -------  -------  -------  -------
  SYS1      N        N        N        N
  TSO       N        N        N        N



SROONEY  TEST                    1993-04-21 -          -         N N N N

  GROUPID   REVOKE   AUDIT    SPECIAL  OPER
  --------  -------  -------  -------  -------
  TEST      N        N        N        N

 COMMAND ===> _                                              SCROLL ===> PAGE

 F13=Help     F14=         F15=End      F16=         F17=R Find   F18=R Change
 F19=Backward F20=Forward  F21=         F22=Left     F23=Right    F24=Cursor
```

Figure 37. Sample Users and Their Connect Groups Report

The first line shows the user ID, the programmer name, creation date for this profile, date last accessed, time last accessed, and a 4-character combination showing whether the user has the REVOKE, AUDITOR, SPECIAL, or OPERATIONS attribute on a system-wide basis. The second line and the lines thereafter show information about the groups that the user is connected to. For each group, there is a line showing the group ID and what attributes apply for this user on a group basis, showing the REVOKE, AUDITOR, SPECIAL, and OPERATIONS attributes as showed by the headings.

The report gives an auditor a fast means of checking what groups a user is connected to (that is, what tasks this user is supposed to perform). You can also see what special authorities apply for this user both on a system level and on a group level. Naturally, you should check from time to time to see that the system-level SPECIAL users have not increased and that you have no or very few OPERATIONS users. Also, you could check users that have not logged on to the system and users that are revoked.

Groups and Connected Users: This is a large report that looks a bit crowded when you first look at it. The following information is shown for each user to group connection: Group name, programmer name, user ID, the owner of the user profile, user profile creation date, user last access date, user last access time, and whether the user is revoked. The report is sorted on group name and user ID.

Because the number of fields in this report, you will have to scroll left and right to see all the information about a user, but for most purposes the leftmost part of the report should be enough. What you are probably interested in is which users are connected to a given group, whether those users belong there, and whether the ownership is correct. You may also check for users that have never logged on, but the compressed user profile report is better for that purpose. Use the BROWSE mode for fast search of groups of interest and to find information.

All Occurrences of a User ID or Group Name: Figure 38 shows you an extract of a report of all occurrences of the group SYS1 in the RACF database.

```
REPORT ON ALL OCCURRENCES OF THE NAME SYS1

                                                                CLASS/
                                                                GROUP/
WHERE FOUND          RESOURCE NAME / INSTALLATION DATA           USER
-------------------  ------------------------------------------  --------
CONNECT OWNER        AARON                                       TEST
CONNECT OWNER        USER2                                       TSO
DATA SET ACC. LIST   SYS1.*                                      ALTER
DATA SET ACC. LIST   SYS1.HASPACE                                UPDATE
DATA SET ACC. LIST   SYS1.HASPCKPT                               UPDATE
DATA SET ACC. LIST   SYS1.LINKLIB                                UPDATE
DATA SET ACC. LIST   SYS1.RACFMXA                                UPDATE
DATA SET OWNER       ACFNCP.*
DATA SET OWNER       AMS.*
DATA SET OWNER       APL2.*
DATA SET OWNER       CATALOG.*
GENERAL RES. OWNER   ICHDSM00                                    PROGRAM
GENERAL RES. OWNER   MXXE83                                      DASDVOL
GROUP OWNER          ACFNCP                                      SYS1
GROUP SUBGROUP       ACFNCP
USER CONNECT DATA G                                              ALLMOND
USER DEFAULT GROUP   DFHSM OPERATOR ID                           HSMOPER
USERID OWNER         TT                                          AARON
```

Figure 38. Sample Occurrences of the Group SYS1 (Extracts) Report

The fields shown in the output are so varied that it is not possible to describe the contents of the different fields in the headings.

Frequently, administrators are asked to pattern a user or a group by using an existing profile as a model. IRRUT100 has so far been the only available tool to

obtain exactly in which profiles that user ID or group is to be found. However, IRRUT100 does not sort the profiles in any order, so you then have to break down the output from the utility to see all the access lists, all the groups, and so on where a user ID is defined.

This report shows you all the IRRUT100 information and some additional information sorted so that you can see all the profiles where your user or group is defined. With a little creativity, you may even use the report to build all the commands to pattern another user or group with the same authorities or scope.

Table 1 shows what the contents of the different fields are, depending on the contents of the “WHERE FOUND” field.

Table 1. Interpreting the Option 11 Report

WHERE FOUND	RESOURCE NAME / INSTALLATION DATA	CLASS/GROUP/USER
CONNECT OWNER	User ID	Default Group
DATA SET ACC. LIST	Data Set Name	Access Allowed
DATA SET NOTIFY ID	Data set name	-
DATA SET OWNER	Data set name	-
DATA SET RESOWNER	Data set name	-
DS. COND. ACC. LIST	Data set name	Type of checking (PROGRAM, CONSOLE, TERMINAL or JESINPUT)
GEN. RES. ACC. LIST	General resource name	Resource class
GEN. RES. COND. ACC	General resource name	Resource class
GEN. RES. NOTIFY ID	General resource name	Resource class
GENERAL RES. OWNER	General resource name	Resource class
GROUP	Group installation data	Superior group
GROUP OWNER	Group name	Superior group
GROUP SUBGROUP	Name of the subgroup	-
OPERPARM DEFGROUP	Console operator ID	-
USER CICS DATA	-	-
USER CICS OPER CLAS	-	-
USER CONNECT DATA G For group report	User ID	-
USER CONNECT DATA U For user report	Name of connect group	-
USER CONNECT GROUP For group report	User ID	-
USER CONNECT GROUP For user report	Name of connect group	-
USER DEFAULT GROUP	Programmer name	User ID
USER OPERPARM	Default group associated with operator	User ID
USER TSO DATA	User account number	User LOGON procedure
USERID OWNER	Programmer name	User ID
USERID	Programmer name	Default group

6.1.5 Remove Undefined Users and Groups from Access Lists

This function is also called “profile clean-up” and goes through all access lists to verify that each entry is either a valid user ID, group or “*” (all RACF defined users). Since the process takes a while to run for large databases, there are two selections on the panel: one for cleaning the data set access lists, and the

other for cleaning general resource access lists. If you just press Enter, the data set access lists will be processed.

The resulting commands from the clean-up operation are be written to a data set that is named hlq.COMMAND.OUTPUT, where hlq is equal to your user ID. The commands are executed directly out of this data set, or if the resulting number of commands is large (as suggested by the ending message), you should create a job to run the commands under TSO in batch. The benefits of running the commands in batch are that you do not tie up your terminal while the commands are executing, and you are provided with a log for what was done and can check the log for possible errors.

Note: The commands for both data sets and general resources are written to the same data set, so you should either save the commands before executing the other option, or change the REXX EXECs (RACFPEDS and RACFPEGR) to write the results to separate data sets.

Appendix A. Sample CLIST for Starting the Report Application

```
PROC 0 PANEL(DB23PRIM)                                                  00010000
/*********************************************************************  00020000
/*     DB2/ISPF/PDF INVOCATION                                          00030000
/*     A COPY OF CLIST DB23 - USED FOR STARTING THE RACF REORTING       00050203
/*********************************************************************  00050400
WRITE ************************************************************** 00050500
WRITE *                                                              * 00050600
WRITE *    THIS IS A DB2 2.3 SYSTEM WITH QMF 3.1.1.          5/93    * 00050700
WRITE *                                                              * 00050800
WRITE ************************************************************** 00051100
CONTROL   NOMSG NOPROMPT NOLIST NOCONLIST NOSYMLIST NOFLUSH MAIN        00051200
PROFILE   MODE WTPMSG MSGID                                             00051300
/*********************************************************************/ 00051400
/*                                                                   */ 00052000
/* NOTE: SYSPROC IS FREED AND REALLOCATED TO INCLUDE THE DB2 AND QMF */ 00052100
/*       DATASET AND THE XXXXXXXX.YYYYYYYY.EXEC LIBRARY WHICH        */ 00052200
/*       CONTAINS THE PACKAGE EXECS. THIS MAY RESULT IN A DIFFERENT  */ 00052500
/*       CONCATENATION THAN EXISTED BEFORE THIS CLIST WAS INVOKED.   */ 00053000
/*                                                                   */ 00054000
/*********************************************************************/ 00055000
CONTROL NOFLUSH NOMSG MAIN                                              00056000
PROFILE MODE WTPMSG MSGID                                               00057000
FREE FILE(ISPLLIB,ISPPLIB,ISPMLIB,ISPTLIB,ISPSLIB, +                    00058000
          ISPPROF,ISPTABL,SMPTABL)                                      00059000
FREE FI(SYSPROC)                                                        00060000
FREE FI(DSQEDIT)                                                        00070000
FREE FI(DSQSPILL)                                                       00080000
  /*****************************************************************/ + 00090000
  /*                  SYSPROC                                      */ + 00100000
  /*****************************************************************/ + 00110000
IF &SYSDSN('&SYSUID..LOGON.CLIST') NE &STR(OK) THEN +                   00120000
ALLOC FI(SYSPROC) SHR DA( +                                             00130000
                         'DSN230.NEW.DSNTEMP' +                         00140000
                         'DSN230.DSNCLIST' +                            00150000
                         'QMF.V311.DSQCLSTE'    +                       00160000
                         'DSN230.LOCAL.CLIST'    +                      00161000
                         'xxxxxxxx.yyyyyyyy.EXEC'    +                  00166100
                         )                                              00167000
 ELSE +                                                                 00168000
ALLOC FI(SYSPROC) SHR DA( +                                             00169000
                         '&SYSUID..LOGON.CLIST' +                       00170000
                         'DSN230.NEW.DSNTEMP' +                         00180000
                         'DSN230.DSNCLIST' +                            00190000
                         'QMF.V311.DSQCLSTE'    +                       00200000
                         'DSN230.LOCAL.CLIST'    +                      00210000
                         'xxxxxxxx.yyyyyyyy.EXEC'    +                  00261000
                         )                                              00270000
    END                                                                 00280000
  ALLOC FI(SYSEXEC) SHR DA( +                                           00290000
                         'QMF.V311.DSQEXECE'    +                       00300000
                           )                                            00310000
  ALLOC FI(DSQPNLE) SHR DA( +                                           00320000
                         'QMF.V311.DSQPNLE'     +                       00330000
                           )                                            00340000
```

```
/*************************************************************/ +   00350000
/*                   PROFILE                                 */ +   00360000
/*************************************************************/ +   00370000
SET &DSNAME = &SYSUID..ISPF.ISPPROF                                 00380000
ALLOC FI(ISPPROF) SHR  DA('&DSNAME.')                               00390000
IF &LASTCC ¬= 0 THEN +                                              00400000
  DO                                                                00410000
    FREE FI(ISPCRTE)                                                00420000
    CONTROL MSG                                                     00430000
    ATTRIB ISPCRTE DSORG(PO) RECFM(F B) LRECL(80) BLKSIZE(3120)     00440000
    ALLOC DA('&DSNAME.') SP(2,1) TRACKS DIR(2) USING(ISPCRTE) +     00450000
        FI(ISPPROF)                                                 00460000
    IF &LASTCC = 0 THEN +                                           00470000
      WRITE *** ISPF PROFILE DATA SET '&DSNAME.' HAS BEEN CREATED   00480000
    ELSE +                                                          00490000
     DO                                                             00500000
      WRITE  *** UNABLE TO ALLOCATE ISPF PROFILE DATA SET '&DSNAME.' 00510000
      FREE FI(ISPCRTE)                                              00520000
      EXIT CODE(12)                                                 00530000
     END                                                            00540000
    FREE FI(ISPCRTE)                                                00550000
  END                                                               00560000
CONTROL MSG                                                         00570000
IF &PANEL = &STR() THEN +                                           00580000
  SET &PNL = PANEL(ISR@PRIM)                                        00590000
ELSE +                                                              00600000
  SET &PNL = PANEL(&PANEL)                                          00610000
ALLOC FI(ISPTABL) SHR DA('&DSNAME.')                                00620000
ALLOC FI(SMPTABL) SHR DA('&DSNAME.')                                00630000
  /*************************************************************/ + 00640000
  /*                  STEPLIB                                  */ + 00650000
  /*************************************************************/ + 00660000
ALLOC FI(ISPLLIB) SHR DA(   +                                       00670000
                       'SYS1.GDDM.SADMMOD'  +                       00680000
                       'DSN230.DSNEXIT' +                           00690000
                       'DSN230.DSNLOAD' +                           00700000
                       'DSN230.RUNLIB.LOAD'       +                 00710000
                       'QMF.V311.DSQLOAD'         +                 00720000
                       )                                            00760000
  /*************************************************************/ + 00770000
  /*                  ISPPLIB                                  */ + 00780000
  /*************************************************************/ + 00790000
ALLOC FI(ISPPLIB) SHR DA(     +                                     00800000
                       'xxxxxxxx.yyyyyyyy.PANELS'  +                00801005
                       'DSN230.LOCAL.PLIB'     +                    00810000
                       'DSN230.DSNSPFP'       +                     00813000
                       'QMF.V311.DSQPLIBE'    +                     00814000
                       'ISP.V3R5M0.ISPPENU'  +                      00818000
                       'ISR.V3R5M0.ISRPENU'  +                      00819000
                       )                                            00820000
```

```
  /*************************************************************/ + 00830000
  /*                   ISPMLIB                                 */ + 00840000
  /*************************************************************/ + 00850000
ALLOC FI(ISPMLIB) SHR DA( +                                       00860000
                       'DSN230.LOCAL.MLIB'   +                    00870000
                       'DSN230.DSNSPFM' +                         00890000
                       'QMF.V311.DSQMLIBE'   +                    00900000
                       'ISP.V3R5M0.ISPMENU'  +                    00940000
                       'ISR.V3R5M0.ISRMENU'  +                    00950000
                       )                                          00960000
/*************************************************************/ +   00970000
/*                   TABLES                                  */ +   00980000
/*************************************************************/ +   00990000
ALLOC FI(ISPTLIB) SHR DA( +                                       01000000
                       '&DSNAME.'           +                     01010000
                       'ISP.V3R5M0.ISPTENU'  +                    01040000
                       'ISR.V3R5M0.ISRTLIB'  +                    01050000
                       )                                          01060000
/*************************************************************/ +   01070000
/*                   SKELETONS                               */ +   01080000
/*************************************************************/ +   01090000
ALLOC FI(ISPSLIB) SHR DA(          +                              01100000
                       'QMF.V311.DSQSLIBE'   +                    01110000
                       'ISP.V3R5M0.ISPSLIB'  +                    01140000
                       'ISR.V3R5M0.ISRSENU'  +                    01141000
                       )                                          01142000
ALLOC FI(ICQAATAB) SHR DA('ICQ.ICQAATAB')                         01143000
ALLOC FI(ICQANTAB) SHR DA('ICQ.ICQANTAB')                         01144000
ALLOC FI(ICQAPTAB) SHR DA('ICQ.ICQAPTAB')                         01145000
ALLOC FI(ICQAMTAB) SHR DA('ICQ.ICQAMTAB')                         01146000
ALLOC FI(ICQCMTAB) SHR DA('ICQ.ICQCMTAB')                         01147000
/*                                                          */     01148000
 /****** QMF GDDM MAPS */                                         01149000
    ALLOC FI(ADMGGMAP) SHR DA('QMF.V311.DSQMAPE') REUS             01150002
/*                                                          */     01160000
 /****** QMF GDDM FORM */                                         01170000
    ALLOC FI(ADMCFORM) SHR DA('QMF.V311.DSQCHART')                 01180000
/*************************************************************/ +   01190000
/*                   HELP                                    */ +   01200000
/*************************************************************/ +   01210000
  ALLOC FI(SYSHELP) SHR DA( +                                     01220000
         'SYS1.HELP' ) REUSE                                      01230000
/*                                                          */     01240000
 /****** SYSUDUMP DATA SET  */                                    01250000
 /****** DSQUDUMP DATA SET  */                                    01260000
 /****** PLI DUMP DATA SET */                                     01270000
 /****** QMF DEBUG DATA SET */                                    01280000
 /****** QMF PRINT DATA SET */                                    01281000
    ALLOC FI(SYSUDUMP) +                                          01282000
          SYSOUT(T) LRECL(121) BLKSIZE(1210) RECFM(F,B,A) REUSE   01283000
    ALLOC FI(DSQUDUMP) +                                          01284000
          SYSOUT(T) LRECL(125) BLKSIZE(1632) RECFM(V,B,A) REUSE   01285000
    ALLOC FI(PLIDUMP) +                                           01286000
          SYSOUT(T) LRECL(121) BLKSIZE(1210) RECFM(F,B,A) REUSE   01287000
    ALLOC FI(DSQDEBUG) +                                          01288000
          SYSOUT(T) LRECL(121) BLKSIZE(1210) RECFM(F,B,A) REUSE   01289000
    ALLOC FI(DSQPRINT) +                                          01290000
          SYSOUT(T) LRECL(133) BLKSIZE(6118) RECFM(F,B,A) REUSE   01300000
/*                                                          */     01310000
```

```
 /****** QMF DSQEDIT DATA SET */                                          01320000
    ALLOC FI(DSQEDIT) UNIT(SYSDA) +                                       01330000
          LRECL(79) BLKSIZE(4029) RECFM(F,B,A)                            01340000
/*                                                                 */     01350000
 /****** QMF SPILL     */                                                01360000
    ALLOC FI(DSQSPILL) UNIT(SYSDA) SPACE(1,1) +                           01361000
           LRECL(4096) BLKSIZE(4096) RECFM(F) CYL REUSE NEW DELETE        01362000
/*****************************************************************/ +   01363000
/*                  INVOKE ISPF/PDF                              */ +   01364000
/*****************************************************************/ +   01365000
/* ERROR RETURN */                                                       01366000
WRITE                                                                     01367000
WRITE                                                                     01368000
WRITE  ******    NOW ENTERING ISPF/PDF V3.5.0                             01369000
WRITE                                                                     01370000
PDF &PNL                                                                  01380000
EXIT                                                                      01390000
```

Index

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

ITSO Technical Bulletin Evaluation RED000

Enhanced Auditing Using the RACF SMF Data Unload Utility

Publication No. GG24-4453-00

Your feedback is very important to help us maintain the quality of ITSO Bulletins. **Please fill out this questionnaire and return it using one of the following methods:**

- Mail it to the address on the back (postage paid in U.S. only)
- Give it to an IBM marketing representative for mailing
- Fax it to: Your International Access Code + 1 914 432 8246
- Send a note to REDBOOK@VNET.IBM.COM

Please rate on a scale of 1 to 5 the subjects below.
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction	____		
Organization of the book	____	Grammar/punctuation/spelling	____
Accuracy of the information	____	Ease of reading and understanding	____
Relevance of the information	____	Ease of finding information	____
Completeness of the information	____	Level of technical detail	____
Value of illustrations	____	Print quality	____

Please answer the following questions:

a) If you are an employee of IBM or its subsidiaries:

Do you provide billable services for 20% or more of your time? Yes____ No____

Are you in a Services Organization? Yes____ No____

b) Are you working in the USA? Yes____ No____

c) Was the Bulletin published in time for your needs? Yes____ No____

d) Did this Bulletin meet your needs? Yes____ No____

If no, please explain:

_____

_____

What other topics would you like to see in this Bulletin?

_____

_____

What other Technical Bulletins would you like to see published?

_____

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

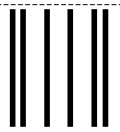
_____ _____
Name Address

_____ _____
Company or Organization

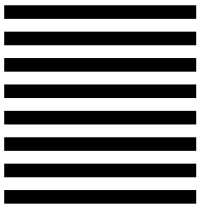
_____ _____
Phone No.

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM International Technical Support Organization
Mail Station P099
522 SOUTH ROAD
POUGHKEEPSIE NY
USA 12601-5400

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

Printed in U.S.A.