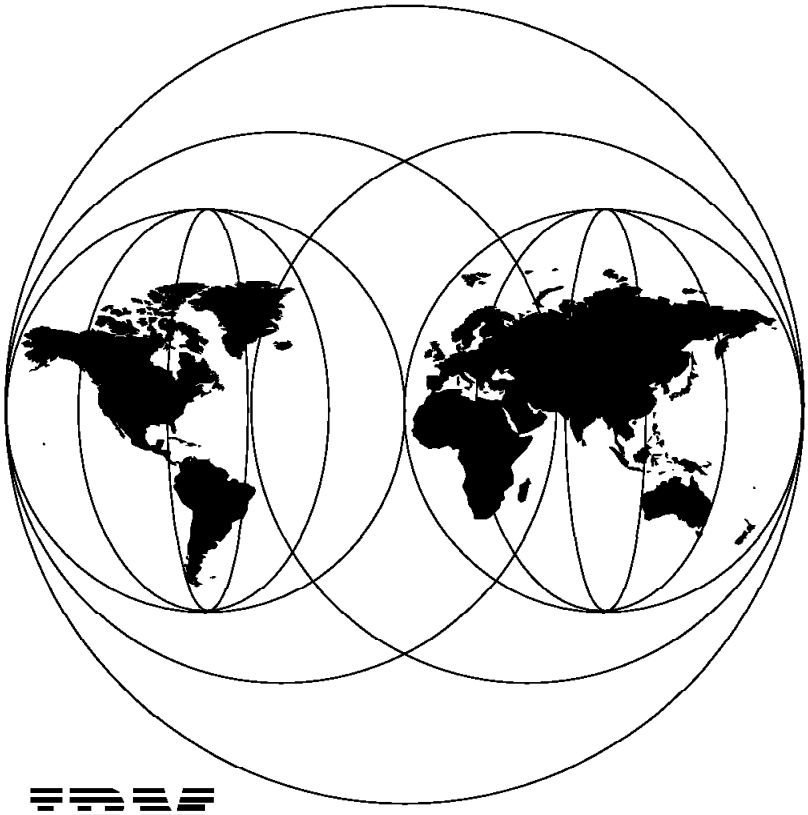
SG24-4820-00

OS/390 Security Server
Audit Tool and Report Application

December 1996



IBM

International Technical Support Organization
Poughkeepsie Center

International Technical Support Organization

SG24-4820-00

OS/390 Security Server
Audit Tool and Report Application

December 1996

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix E, “Special Notices” on page 105.

First Edition (December 1996)

This edition applies to Release Number 1 of OS/390 Security Server, for use with the OS/390 Operating System

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. HYJ Mail Station P099
522 South Road
Poughkeepsie, New York 12601-5400

Contents

Figures

Preface

This document is intended to give data security auditors an overview of the various tools that are available to audit a OS/390 Security Server environment. It describes an application that is used to assist in both OS/390 Security Server administration and auditing. This document also describes 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 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 as the database manager.

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

How This Redbook Is Organized

This redbook contains 115 pages. It 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, “Installing the Audit and Report Application”

  This chapter provides information on the prerequisites necessary to run the Audit and Report Application, as well as how to install the package on your system.

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

  This chapter describes the reports created by the Audit and Report Application and suggests ways in which an auditor or administrator might use these reports.

- Chapter 5, “Extending the Audit and Report Application to Support a Web Browser”

  This chapter describes how to extend the application to be used through a Web Browser. We used a OS/390 Web Server, the DB2 WWW Connection product, coding macros, and HTML pages to generate reports that can be viewed through the use of a Web Browser.

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

This appendix contains a sample CLIST which can be used to start the Audit and Report Application.

- Appendix B, “Sample DB2 WWW Macros and HTML Pages”

  This appendix contains the sample DB2 WWW Connection macros and sample HTML pages used by the Audit and Report Application.

- Appendix C, “Sample REXX Procedure to Add SMF-ID”

  This appendix contains the sample ADDSYSID REXX procedure to add the SMF-ID to the output of the RACF Database Unload Utility.

- Appendix D, “How to Obtain the Audit and Report Application”

  This appendix describes how to obtain the Audit and Report Application.

- Appendix F, “Related Publications”

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

The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization Poughkeepsie Center.

The project leader for this project was:

Cees Kingma

Advisory International Technical Support Specialist for enterprise security in the International Technical Support Organization.

The authors of this document are:

Ricardo Alvarez is a Security Support Specialist in Argentina. He has worked at IBM since 1978 and has 8 years of experience in the security field.

Paul de Graaff is a Security Management Consultant in the Netherlands. He has 10 years of experience in the security field. His areas of expertise include Security on Large Systems, AS/400 and LAN environments. He has worked with IBM since 1989.

Hilding Landén is a Certified Solutions Architect in Sweden. He has 20 years of experience in the security field. He has worked at IBM for 30 years. His areas of expertise include Security and Large Systems. He has written extensively about RACF.

Thanks to Mark Nelson from RACF development for his invaluable contributions to this project.

Comments Welcome

We want our redbooks to be as helpful as possible. Should you have any comments about this or other redbooks, please send us a note at the following address:

redbook@vnet.ibm.com

Your comments are important to us!

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:

- Verify 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 and 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 an entirely 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 ad hoc 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 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 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 ad hoc queries. The alternative is for someone to build an application with a set of predefined reports that can easily be adapted to fit the individual installation.

This brings us to the subject of this redbook, 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 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 and report application* described in this book consists of the following parts:

- An auditing application that uses the ISPF, REXX EXECs, and QMF in OS/390. This application is based on the RACF SMF Data Unload Utility.
- The enhanced reporting application that uses ISPF, REXX EXECs, and QMF in OS/390. This application is based on the RACF Database Unload Utility.

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

In 4.2, “Selecting Reports” on page 29, we explain how to use the enhanced reporting application.

1.1 How to Get Materials Discussed in This Redbook

The materials discussed in this redbook will be made available to you through the Internet. A package will be made available through the Large Scale Computing FTP server. See Appendix D, “How to Obtain the Audit and Report Application” on page 103 for more details on how to obtain the complete package. The package will be refreshed when required, but the code remains on a “best support” basis.

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 applications that are either supplied with the Resource Access Control Facility (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)
- DFSORT ICETOOL Security Analysis Tool

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 to produce reports by some other means, where the output is then massaged either into a more meaningful report, or into RACF commands that will 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 led through the RACF ISPF panels. For the inexperienced user, the RACF ISPF panels are still the recommended path to take. To see the online 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 preallocated 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, by using the CLIST option, build a CLIST for execution. For example, if you want to change the universal access of all your data set profiles, execute these two commands in sequence:

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

This searches 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 only need to execute the CLIST, and the universal access is changed to NONE for every data set profile.

One of the SEARCH command's few disadvantages is that it executes 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 a user ID supplied to the program by an authorized user. As with most programs, simplistic input normally means simplistic output.

To use the IRRUT100, you need 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 it only identifies the occurrences of the user ID or group. 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 it must be used with judgement so as not to affect performance in a negative way. The output will usually 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), or even 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 backups or the database since the Assembler macros used to read the RACF database only work on the live databases.

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. This is not a good idea unless it is done after prime shift, because IRRUT100 can affect performance of the system.

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.

JCL samples of how to run this new utility program can be found in SYS1.SAMPLIB(RACJCL).

The samples also show how the output of the RACF Database Unload Utility is 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 ad hoc queries on the data. Refer to Figure 3 for a sample query.

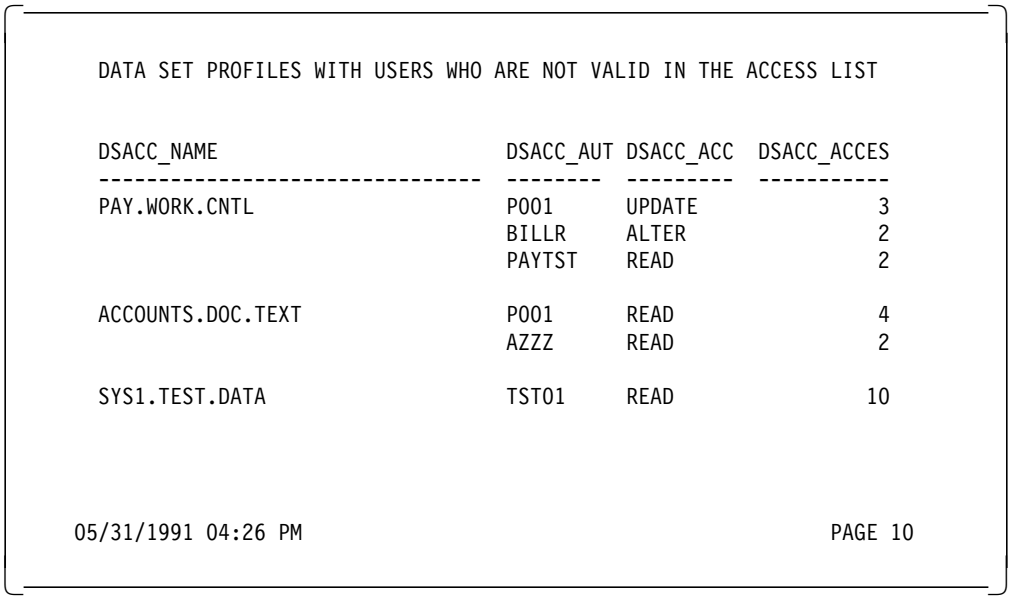
```
 Description: Check all of the data set standard access lists and
              verify that each user ID is a valid user or
              group ID

 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
           )
   AND
      X.DSACC_AUTH_ID¬=’*’
  ORDER BY 1
             ;
```

Figure 3. Sample SQL Query

Figure 4 shows the results from the SQL query.

Note: Not all the 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 subcommands.

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 R190  ORIGIN:   SETROPTS          DATASET  YES   YES  NO  YES YES  YES            DFLT
                      TERMUACC: READ              USER               NO
                      CMNDVIOL: YES               GROUP              NO
                      LOGSPEC:  YES               RVARSMBR YES   NO   NO  YES YES  YES            DFLT
                      RACINIT:  STATS             RACFVARS YES   NO   NO  YES YES            YES  DFLT
                      ADSP:     ACTIVE            SECLABEL YES   NO   NO  YES YES  YES            DFLT
                      REALDSN:  NO                DASDVOL  NO    NO   NO  YES YES  YES            DFLT
                      JES:                        GDASDVOL NO    NO   NO                          DFLT
                        BATCHALLRACF              TAPEVOL  YES   NO   NO  YES YES  YES            DFLT
                        XBMALLRACF                TERMINAL YES   NO   NO  YES YES  YES            DFLT
                        EARLYVERIFY               GTERMINL YES   NO   NO                          DFLT
                                                  APPL     NO    NO   NO  YES YES  YES            DFLT
                      TAPEDSN:  NO                TIMS     NO    NO   NO  YES YES  YES            DFLT
                      PROT-ALL: NO                GIMS     NO    NO   NO                          DFLT
                      PROGCTL:  NO                AIMS     NO    NO   NO  YES YES  YES            DFLT
                      OPERAUDIT: NO               TCICSTRN NO    NO   NO YES YES  YES            DFLT
                      ERASE:    YES               GCICSTRN NO    NO   NO                          DFLT
                        NOSECLEVEL                PCICSPSB NO    NO   NO  YES YES  YES            DFLT
                        ALL                       QCICSPSB NO    NO   NO                          DFLT
                      SECLEVELAUDITING INACTIVE   GLOBAL   NO    NO   NO                          DFLT
                      EGN:      INACTIVE          GMBR     NO    NO   NO  YES YES  YES            DFLT
                      SESSIONINTERVAL    30       DSNR     NO    NO   NO  YES YES  YES            DFLT
                      JES B1 SECURITY:            FACILITY NO    NO   NO  YES YES  YES            DFLT
                           NJEUSERID:  UNKUSER    VMMDISK  NO    NO   NO  YES YES  YES            DFLT
                        UNDEFINEDUSER: ++++++++   VMRDR    NO    NO   NO  YES YES  YES            DFLT
                      DEFAULT LANGUAGE CODES:     SECDATA  NO    NO   NO                          DFLT
                                PRIMARY CODE: ENU PROGRAM  NO    NO   NO                          DFLT
                              SECONDARY CODE: ENU APPCLU   NO    NO   NO  YES YES  YES            DFLT
                     APPLAUDIT:  YES
                                                  JESJOBS  YES   NO   NO  YES YES  YES            DFLT
                                                  JESINPUT YES   NO   NO  YES YES  YES            DFLT
                                                  CONSOLE  YES   NO   NO  YES YES  YES       YES  DFLT
                                                  TEMPDSN  YES   NO   NO  YES YES  YES            DFLT
                                                  DIRAUTH  YES   NO   NO  YES YES  YES            DFLT
                                                  SURROGAT YES   NO   NO  YES YES  YES            DFLT
                                                  NODMBR   YES   NO   NO  YES YES  YES            DFLT
                                                  NODES    YES   NO   NO  YES YES            YES  DFLT
                                          OTHER OPTIONS -
                                            'LIST OF GROUPS' 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
                                         --------------- ----- R E S O U R C E   S T A T I S T I C S ---------------------
   USER/     NAME              ---- JOB/LOGON ----                          ------------ I N T E N T S ------------
   *JOB                       SUCCESS VIOLATION   SUCCESS   WAR NING VIOLATION     ALTER   CONTROL    UPDATE      READ     TOTAL
*CLRMANB                            1         0         0         0         0         0         0         0         0         0
 IBMUSER                            7         0         0         0         0         0         0         0         0         0
 RACUSR1                            0         0         1         0         0         0         0         0         0         1
 RACUSR1    MARY BAILEY             0         0        21         0         0        21         0         0         0        21
 RACUSR2                            0         0         1         0         0         0         0         0         0         1
 RACUSR2    MARY   PURCELL          0         0         1         0         0         1         0         0         0         1
 RACUSR3                            0         0         1         0         0         0         0         0         0         1
 RACUSR3    HARRIET BIRD            0         0         1         0         0         1         0         0         0         1
 RACUSR4                            0         0         1         0         0         0         0         0         0         1
 RACUSR4    JOHN H. BUKOWSKI        0         0         1         0         0         1         0         0         0         1
 RACUSR5                            0         0         1         0         0         0         0         0         0         1
 RACUSR5    MELANIE WILKES          0         0         1         0         0         1         0         0         0         1
 RACUSR6                            0         0         1         0         0         0         0         0         0         1
 RACUSR6    FRED PRETOCK            0         0         1         0         0         1         0         0         0         1
 RACUSR7                            0         0         1         0         0         0         0         0         0         1
 RACUSR7    HESTER WILSON           0         0         1         0         0         1         0         0         0         1
 SLCUSRD1                           0         0         1         0         0         0         0         0         1         1
 SLCUSRD5                           0         0         0         0         1         0         0         0         1         1
 ACCUMULATED TOTALS -               8         0        35         0         1        27         0         0         2        36
 PERCENTAGE OF TOTAL ACCESSES -                        97 %       0 %       3 %      75 %       0 %       0 %       6 %
 UNDEFINED USERS (JOBS) ONLY
 ACCUMULATED TOTALS -               1         0         0         0         0         0         0         0         0         0
 PERCENTAGE OF TOTAL ACCESSES -                         0 %       0 %       0 %       0 %       0 %       0 %       0 %
```

Figure 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 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 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 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  User       RACF     Account                          Job
  id    group      userid   field1    Date        Time       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

2.10 DFSORT ICETOOL Security Analysis Tools

DFSORT's ICETOOL utility, introduced in R11.1 and enhanced in R12 and R13, provides a fast and efficient means of analyzing and producing reports from IRRDBU00 and IRRADU00 output. ICETOOL is an easy-to-use front-end for DFSORT that allows the use of DFSORT capabilities (for example, field, bit-level and substring filtering, multiple output, editing, lookup and change, and so on) while adding powerful new capabilities through twelve operators (COPY, COUNT, DEFAULTS, DISPLAY, MODE, OCCURS, RANGE, SELECT, SORT, STATS, UNIQUE and VERIFY). Any number or combination of these operators can be used in a single ICETOOL step.

As shown in the examples that follow, ICETOOL's DISPLAY and OCCURS operators make it easy to create reports from RACF data with titles, headings, page numbers and date and time stamps. Although not shown in these examples, DISPLAY reports can also contain statistics (maximum, minimum, average, total) and sections. Note that both reports could have been created in the same ICETOOL step; they are shown separately here to make it easier to explain them.

You can find complete details about DFSORT and ICETOOL in *DFSORT Application Programming Guide.*

Refer to Figure 12 on page 18 for a ICETOOL JCL and Statements sample.

```
//EVNTRPT JOB ...
//SHOWIT  EXEC PGM=ICETOOL
//TOOLMSG DD SYSOUT=*
//DFSMSG  DD SYSOUT=*
//IN       DD DSN=MARKN.TYPE80.IRRADU00,DISP=SHR
//TEMP     DD DSN=&T1,DISP=(,PASS),SPACE=(CYL,(20,5))
//EVENTS   DD SYSOUT=*
//TOOLIN  DD *
*********************************************
* Find all of the records which are applicable *
* to a specific User ID.                      *
*********************************************
 COPY    FROM(IN) TO(TEMP) USING(SELU)
 DISPLAY FROM(TEMP) LIST(EVENTS) -
         PAGE TITLE('Events for User MARKN') -
         DATE(4MD-) TIME(12:) -
         ON(63,8,CH)  HEADER('User ID') -
         ON(5,8,CH)   HEADER('Event') -
         ON(14,8,CH)  HEADER('Qualifier') -
         ON(23,8,CH)  HEADER('Time') -
         ON(32,10,CH) HEADER('Date') -
         ON(43,4,CH)  HEADER('System') -
         ON(175,8,CH) HEADER('Terminal') -
         ON(184,8,CH) HEADER('Jobname') -
         BLANK
/*
//SELUCNTL DD *
  INCLUDE COND=(5,8,CH,EQ,C'ACCESS',AND,
                63,8,CH,EQ,C'MARKN')
  OPTION   VLSHRT
/*
```

Figure 12. ICETOOL JCL and Statements for Events Report

The report is created in a single step using two ICETOOL operators, COPY and DISPLAY. Here is how:

1. The **COPY** operator is used to select the records for the report and copy them to a temporary data set to be used for the DISPLAY operator. **FROM** specifies the ddname (IN) of the input data set. **TO** specifies the ddname (TEMP) of the output data set. Any ddname can be used for FROM and TO. **USING** specifies the ddname (SELUCNTL) of a data set containing DFSORT control statements. 'CNTL' is always appended to the four characters specified for USING.

   The **INCLUDE** statement in SELUCNTL selects only those records which have the string 'ACCESS ' in positions 8 to 15 AND the string 'MARKN ' in positions 63 to 70. Because the strings are shorter than the fields, DFSORT pads the strings with blanks at the end. The **OPTION VLSHRT** statement tells DFSORT to continue operating even though it finds variable length input records that are too short to contain all the **INCLUDE** fields.

2. The **DISPLAY** operator is used to create the report from the records selected by the COPY operator. DISPLAY produces simple, tailored or sectioned reports in column format with titles, page numbers, date and time stamps, headings, and statistics, as needed. ICETOOL does all of the work of formatting the report elements you specify.

FROM specifies the ddname (TEMP) of the temporary data set created by the preceding COPY operator. **LIST** specifies the ddname (EVENTS) of the report data set.

PAGE, **TITLE**, **DATE**, and **TIME** specify the information to appear in the title line at the beginning of each page. The elements of the title line are printed in the order specified. The date and time stamps selected are only two of many possibilities.

Each **ON** and **HEADER** pair specify a field to appear as a data column in the report, and the heading to be used for that field. The data columns appear in the order specified. Each field is described by its position, length and format. DISPLAY supports binary (BI), fixed-point (FI), packed decimal (PD), zoned decimal (ZD), floating sign (FS) and character (CH) formats. Since IRRADU00 and IRRDBU00 fields always consist of character data, format CH can be used.

BLANK specifies that ICETOOL is to adjust the width for each column automatically according to the size of its data and heading.

Figure 13 shows a portion of the output that might be produced by this ICETOOL job.

```
- 1 -      Events for User MARKN        1996-02-29        05:14:49 pm

User ID  Event    Qualifi  Time      Date        System  Term  Jobname
-------  ------   -------  --------  ----------  ------  ----  -------
MARKN    ACCESS   SUCCESS  15:49:59  1996-02-08  IM13    LOC9  MARKN
MARKN    ACCESS   SUCCESS  15:50:27  1996-02-08  IM13    LOC9  MARKN
MARKN    ACCESS   SUCCESS  15:50:27  1996-02-08  IM13    LOC9  MARKN
```

Figure 13. Part of Events Report (in EVENTS)

In Figure 14 on page 20 ICETOOL is used to create a report from IRRADU00 data, that lists all terminals at which more than three incorrect passwords were entered in a single day. The ICETOOL statements shown are similar to those shown in Figure 12 on page 18.

```
*************************************************************
* Find all of the terminals from which an excessive number of *
* logons with incorrect passwords have been attempted.        *
*************************************************************
 COPY   FROM(IN) TO(TEMP) USING(LOGF)
 OCCURS FROM(TEMP) LIST(TERMS) -
        DATE -
        TITLE('Terminals with Excessive Incorrect Passwords')-
        PAGE -
        BLANK -
        ON(32,10,CH) HEADER('Date') -
        ON(175,8,CH) HEADER('Terminal ID') -
        ON(VALCNT)   HEADER('Number of Incorrect Passwords') -
        HIGHER(3)
/*
//LOGFCNTL DD *
 INCLUDE COND=(5,8,CH,EQ,C'JOBINIT',AND,
               14,8,CH,EQ,C'INVPSWD')
 OPTION   VLSHRT
/*
```

Figure 14. ICETOOL Statements for Terminals Report

The report is created in a single step using two ICETOOL operators, COPY and OCCURS. Here is how:

1. The **COPY** operator is used to select the records for the report and copy them to a temporary data set to be used for the OCCURS operator. In this case, LOGFCNTL contains the DFSORT **INCLUDE** statement to select the needed records.
2. The **OCCURS** operator is used to create the report from the records selected by the COPY operator. OCCURS, like DISPLAY, produces simple or tailored reports in column format with titles, page numbers, date and time stamps and headings, as needed. However, OCCURS counts the number of times each field value occurs, limits the values shown to those for which the value count meets specified criteria (HIGHER(n), LOWER(n), EQUAL(n), ALLDUPS or NODUPS), and can print the value counts.

   In this case, the **ON** fields specify that the report is to consist of unique Terminal ID and Date values and their counts, but **HIGHER** limits the values shown to those for which the Terminal ID and Date is found more than three times. Thus, the values printed represent the terminals with more than three failed logons in a single day.

Figure 15 on page 21 shows a portion of the output that might be produced by this ICETOOL job.

```
04/25/96        Terminals with Excessive Incorrect Passwords

Date         Terminal ID   Number of Incorrect Passwords
----------   -----------   -----------------------------
1996-04-03   P4622212                                 7
1996-04-03   P4622600                                 9
1996-04-05   TERM0001                                 4
```

Figure 15. Part of Terminals Report (in TERMS)

Both IRRADU00 and IRRDBU00 create records of variable length. Variable length records always start with a 4-byte record descriptor word (RDW) describing the length of the record. For DFSORT and ICETOOL, position 1 specifies the RDW and position 5 specifies the beginning of the data. However, the IRRADU00 and IRRDBU00 fields described in *OS/390 Security Server (RACF) Macros and Interfaces* start with the data, that is, they do not include the RDW. Therefore, you must add 4 to any position identified for IRRADU00 and IRRDBU00 fields.

For example, the field for the user ID associated with an event is defined in *OS/390 Security Server (RACF) Macros and Interfaces* as beginning at position 59. So 63 (59 + 4) would be used for that position in both the DFSORT **INCLUDE** statement and the ICETOOL **ON** operand, as in Figure 12 on page 18.

Chapter 3. Installing the Audit and Report Application

This chapter discusses the prerequisites for the Audit and Report Application and the steps necessary to install it. Refer to 1.1, “How to Get Materials Discussed in This Redbook” on page 2 for information on how to obtain a copy of the Audit and Report Application.

3.1 Description of the Audit and Report Application

The Audit and Report Application is based on the Interactive System Productivity Facility (ISPF) and guides the user through a set of panels. The panels offer predefined reports and the means of limiting the amount of output data. The object of auditing is often to try to find the things that are out of the ordinary, which is why 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 produced by 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 reports.

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

3.2 Prerequisites for the Audit and Report Application

The Audit and Report Application requires the following products:

RACF 2.x or the OS/390 Security Server

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 Audit and Report Application using other versions of the above program products. For QMF, you need Version 3 Release 1.1, since this is the first release that includes the REXX callable interface.

The installation of the Audit and Report Application does not require any modifications to be done to your operating system or the RACF database.

3.3 Installing the Audit and Report Application

The application consists of the following data sets:

userid.RACF.EXEC

Contains the REXX programs that drive the whole application.

userid.RACF.PANELS

Contains the ISPF panels and the help texts for the application.

userid.RACF.EXP.DATA

Contains information used to control the installation of QMF resources.

userid.RACF.QUERY

Contains the exported QMF queries.

userid.RACF.PROC

Contains the exported QMF procedures.

userid.RACF.FORM

Contains the exported QMF forms.

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. You might want to concatenate your PANELS data set in front of your other panel data sets. The TSO procedure which you will be using should include the necessary data sets and specifications to allow you to run DB2 and QMF.
2. The *Audit and Report Application base panel*, RACF01 (Figure 16 on page 25) is the panel from which you choose the reports you wish to produce. The application is started by entering the selection (for example ″rr″) that your installation has chosen. The selection can either be made visible on your primary selection panel or can be hidden so that only a limited number of people know about it. Assuming that you have chosen ″rr″ to be your selection, then there should be an entry like the one below on your primary selection panel.

   ```
   rr,'cmd(%racf01)'
   ```

   Of course you should have your systems programmer define the panel so that all combinations of capital letters and lower case letters are accepted.

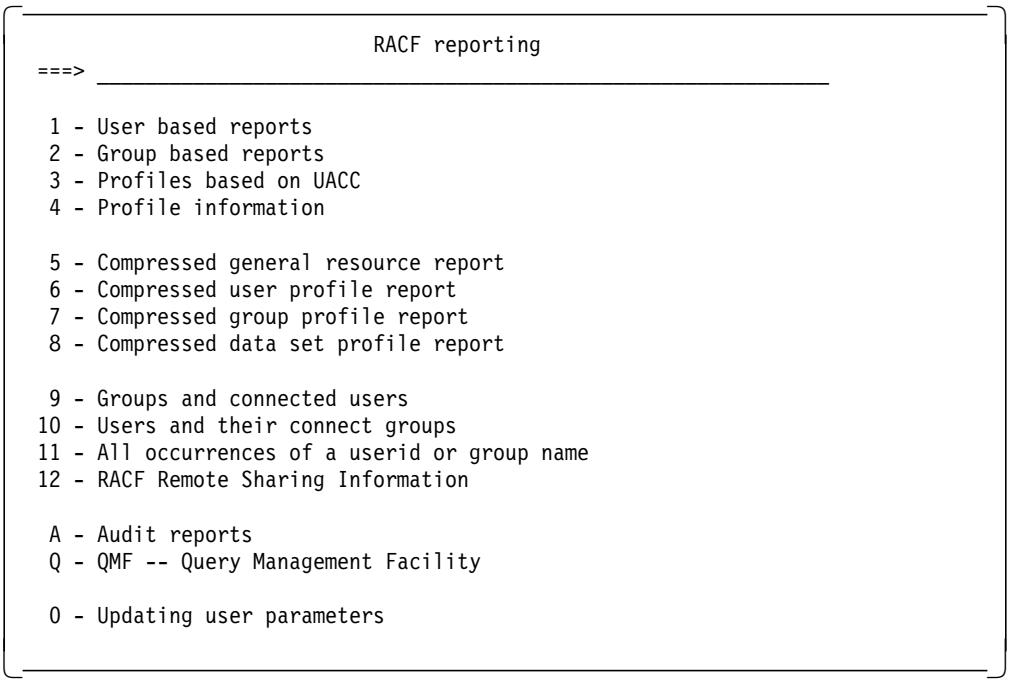


Figure 16. Audit and Report Application Base Panel - RACF01

3. On the RACF01 panel, enter the INSTALL command which will take you to the RACFIMPO panel shown in Figure 17. On this panel, enter the names of the EXP.DATA, QUERY, PROC, and FORM data sets that you have previously received.

   The default assumption is that your data sets have names in which 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 command, and press Enter.

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

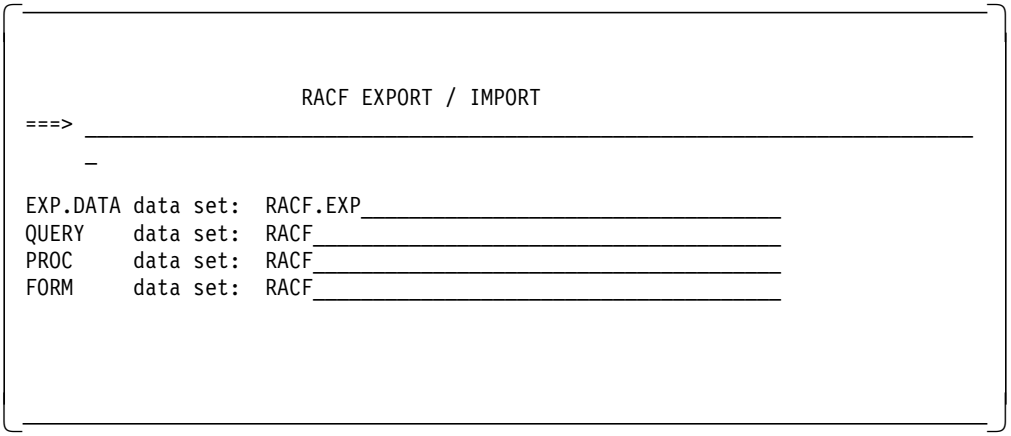


Figure 17. RACFIMPO Panel

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 to correct them or contact

someone who can help you. After the IMPORT is done, you will be back at the RACFIMPO panel. Press PF3 to return to the base panel. Select **0** to update your user parameters. The panel ID is RACFPARM and is shown in Figure 18 on page 26.

```
                              RACF reporting
 ===> ____________________________________________________________

 DB2 subsystem ID  :  DB23__

 RACF Database report

 QMF proc. creator :  HILDING_      Prefix of QMF procedures
 RACF table creator:  GRAAFF_       Prefix of DB2 tables

 RACF Audit report

 QMF proc. creator :  HILDING_      Prefix of QMF procedures
 RACF table creator:  ALVAREZ_      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 18. RACFPARM Panel

Please update the parameters with information relevant to your installation. If you have done the INSTALL step, your user ID should be entered as the QMF procedures creator for both the RACF database reports and the RACF audit reports. The prefixes 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 (depending on who built and named those tables).

The installation defaults for the QMF procedure creator user IDs, the DB2 table creator user IDs, and the DB2 subsystem name are found in the "***userid***.RACF.EXEC" data set in the RACFSQMF member. 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. Using normal QMF output has the advantage of letting you use QMF facilities directly from the output panel as well as enabling you to print your output report directly.

5. Having finished the preceding steps, you are ready to start using the Audit and Report 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 by which you use CLISTs (or REXX) to allocate the necessary data sets.

Appendix A, “Sample CLIST for Starting the Report Application” on page 79, 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 can 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” selection. The “rr” selection takes you to the RACF01 panel but QMF is started before the RACF01 panel is shown. This fact may explain why there is a certain delay before the initial panel is shown.

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 the 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 your “print” key to print the reports that you are producing. The CLIST in Appendix A, “Sample CLIST for Starting the Report Application” on page 79, 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 Audit and Report Application and Sample Reports

This section describes how to use the Audit and Report 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

This section describes the various reports that you can obtain with the reporting application. These reports are selected through selections **1** through **A** on the auditing application base panel, as shown in Figure 19.

```
                          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 - Compressed OMVS profile report

10 - Groups and connected users
11 - Users and their connect group
12 - All occurrences of a user ID or group name

 A - Audit reports
 Q - QMF -- Query Management Facility
 U - Updating user parameters
```

Figure 19. RACF Reporting Main Reports Panel

The base panel includes the following major sections:

- User-based reports
- Group-based reports

- Profile-based reports
- RRSF-based reports
- Summary reports
- User segment information
- Audit reports

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 (sometimes referred to as a “wild card” character and not the asterisk (*).

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.

4.2.1 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 20. 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 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 the RRSF profiles applicable to your selected user.

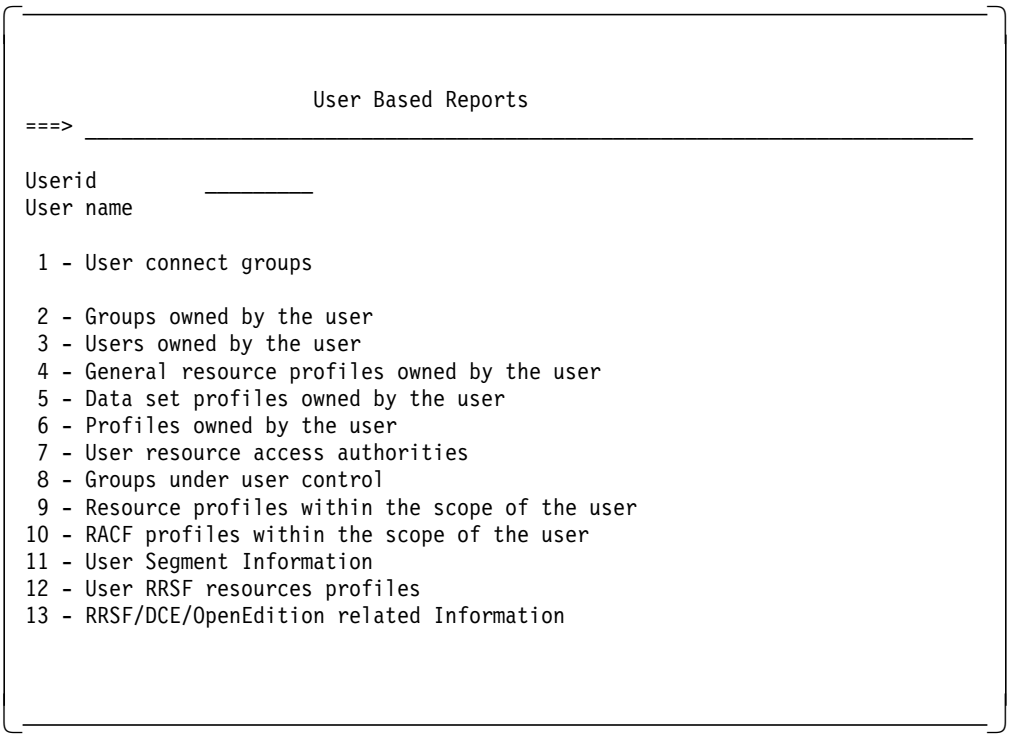


Figure 20. RACFUS01 User-Based Reports Panel

Depending on your choice of output (QMF or BROWSE), there is also a difference in what you can do with your reports. BROWSE lets you use FIND commands and scroll up, down, and sideways; a 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: This report 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 can use this report to verify that a user is not connected to groups that represent duties which that user 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 can be used to obtain which part of the group structure is under a particular user′s control and if this is in line with 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 non-data 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.

Data Set 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.

```
RACF PROFILES OWNED BY HILDING


CLASS     UACC      RESOURCE
--------  --------  ----------------------
DATASET   READ      HILDING.RACF*.**
DATASET   NONE      HILDING.**
```

Figure 21. Data Set Profiles Owned by the User

Profiles Owned by the User: This report lists all the profiles that your chosen user owns. The report is not limited to resources, but also 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.

```
RESOURCE ACCESS REPORT FOR HILDING

CLASS                                    ACCESS
NAME      PROFILE NAME                   ALLOWED   REASON    DB2 TABLE
--------++---------------------        +--------++--------++----------
DATASET   SYS1.KT210.MSG                 READ      UACC      DS_BD
DATASET   SYS1.LINKLIB                   READ      UACC      DS_BD
DATASET   TARGSMP.*.**                   ALTER     UACC      DS_BD
DATASET   TARGSYS.*.**                   ALTER     UACC      DS_BD
DATASET   TPNS.*.**                      ALTER     UACC      DS_BD
DATASET   TPNS4.*.**                     ALTER     UACC      DS_BD
DATASET   USER.*.**                      ALTER     UACC      DS_BD
DATASET   VSAPL.*.**                     ALTER     UACC      DS_BD
DATASET   VSF2.*.**                      ALTER     UACC      DS_BD
DATASET   VSPASCAL.*.**                  ALTER     UACC      DS_BD
FACILITY  DCEKERN.START.REQUEST          UPDATE    HILDING   GENR_ACCES
FACILITY  DCERO03.ENTITY                 ALTER     HILDING   GENR_ACCES
GCICSTRN  DKMS.CSGM                      UPDATE    *         GENR_ACCES
PROGRAM   SU                             ALTER     HILDING   GENR_ACCES
STARTED   SMFDMP.*                       ALTER     HILDING   GENR_ACCES
```

Figure 22. Profiles Owned by the User

User Resource Access Authorities: This 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 is 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 your resource access authorities? This 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, this 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 was that it would not 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. 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 basically 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 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 access is set to ALTER.

```
RESOURCE PROFILES WITHIN THE SCOPE OF ROBBYM

                                          RESOURCE  ACCESS    ACCESS
RESOURCE NAME                              CLASS    ALLOWED     ID
-----------------------------------------++--------++--------++------
ACCNT#                                    ACCTNUM   READ      ROBBYM
RACF.**                                   OPERCMDS  ALTER     TSO
ATBSDFMU                                  PROGRAM   READ      TSO
DIRECT.ICF                                RRSFDATA  ALTER     ROBBYM
PWSYNC                                    RRSFDATA  ALTER     ROBBYM
RACLINK.DEFINE.ICF                        RRSFDATA  ALTER     ROBBYM
ANTMAIN.**                                STARTED   ALTER     ROBBYM
ASCH.**                                   STARTED   ALTER     ROBBYM
BLSJPRMI.**                               STARTED   ALTER     ROBBYM
BWK.**                                    STARTED   ALTER     ROBBYM
CSF.**                                    STARTED   ALTER     ROBBYM
```

Figure 23. Resource Profiles within the Scope of the User

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.

```
RACF PROFILES WITHIN THE SCOPE OF ROBBYM

RESOURCE
 CLASS    UACC      RESOURCE NAME
--------  --------  ----------------------
DATASET   NONE      ICFSMP.**
DATASET   NONE      ROBBYM.*
GROUP     NONE      ICFSMP
RRSFDATA  READ      DIRECT.ICF
RRSFDATA  READ      PWSYNC
RRSFDATA  NONE      RACLINK.DEFINE.ICF
STARTED   NONE      ANTMAIN.**
STARTED   NONE      ASCH.**
STARTED   NONE      BLSJPRMI.**
```

Figure 24. RACF Profiles within the Scope of the User

User Segment Information: This report lists all the user-defined segments. An auditor or administrator can use this report to verify that a user does not have segments defined that he is not supposed to have.

```
RACF SEGMENTS DEFINED FOR THIS USER PROFILE

USERID    SEGMENT
--------  --------
JORDAN    BASE
          DCE
          OMVS
          TSO
```

Figure 25. User Segment Information

User RRSF Resources Profiles: This report shows those resource profiles defined in the RRSFDATA class 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 shows the user ID, the class name (RRSFDATA), Access Allowed, and the Profile Name.

Profile names have been truncated to 42 characters to avoid scrolling left and right for terminal output. If your profile names are often more than 42 characters long, you just have to change the QMF form specification.

```
RESOURCES PROFILES IN RRSFDATA CLASS
====================================

USERID    CLASS     ACCESS    PROFILE NAME
--------  --------  --------  ------------------------
ROBBYM    RRSFDATA  ALTER     DIRECT.ICF
ROBBYM    RRSFDATA  ALTER     PWSYNC
ROBBYM    RRSFDATA  ALTER     RACLINK.DEFINE.ICF
```

Figure 26. User RRSF Resources Profiles

RRSF/DCE/OpenEdition-Related Information: The OS/390 Security Server includes support to enable RACF and DCE to work together and to provide users with support for single sign-on in this environment. DCE includes two utility programs (mvsexpt and mvsimpt) that let a security administrator define an existing RACF user in DCE or the other way around. The net result of using the utility programs is that a user who has logged into DCE can be identified under his RACF user ID as well. On the other hand, a user who is running OpenEdition and is identified to RACF will be logged into DCE if he needs access to DCE resources. The necessary information is stored in the DCE Security Server, the DCE segment of the RACF user profile and the general resource class known as DCEUUIDS.

This process is called cross-linking and it allows interoperability and single sign-on to work.

When choosing this option, the following panel will be displayed :

```
                Report on RRSF / DCE / OpenEdition information
===> ____________________________________________________________

 1 - Show all users with a DCE segment
 2 - Show all DCE users who have no DCEUUIDS profile
 3 - Show all DCE users who are not OpneEdition users
 4 - Show all OpenEdition users
 5 - Show RRSF user information (system wide)
```

Figure 27. RACFUDCE User-Based DCE/OPENEDITION Panel

Show All Users with a DCE Segment: The report shows the RACF user ID, the full user name, the DCE UUID, the home cell, the home UUID and the OMVS user ID.

```
 RACF                    OMVS
USERID    NAME           UID  UUID FOR THE USER   UUID FOR THE HOME CELL
--------  ---------   -------  -----------------   ----------------------
#ROOT#    ########       458
AIXUSER   AIXUSER        206
ALLMOND   ALLMOND          0
BOCHE     BOCHE            0
BPXBATCH  ########         8
BPXROOT   ########         0
CAPTEST   ########        99
CONWAY    CONWAY           0
DAYKA     DAYKA            0  00000088-6a5d-2...  05145c00-c0ee-1c8f-aad.
DAYRAC1   DAYRAC1        801  000000a9-be30-21..  05145c00-c0ee-1c8f-aa..
DAYRAC2   DAYRAC2        802  000000aa-be30-21c.  05145c00-c0ee-1c8f-a...
```

Figure 28. Summary Report With All DCE Users Defined in the System

Show All DCE Users Who Have No DCEUUIDS Profile: The report shows all RACF user IDs with DCE segments, but there is no DCEUUIDS profile that contains this user ID in the APPLDATA field of the profile. There can be no cross-linking from DCE to RACF.

Show All DCE Users Who Are Not OpenEditon Users: The report shows all RACF user IDs with DCE segments, but with no OMVS segments. These instances are highly unlikely and are possible administration errors.

Show All OpenEdition Users: This report shows the RACF user ID, the full user name and the Open Edition MVS user ID.

```
OMVS / RACF-USERID RELATED INFORMATION
======================================

   RACF     USER                        OMVS
  USERID    NAME                       USERID
  --------  -------------------  -----------
  ALLMOND   ALLMOND                      5630
  ASSLING   RAINER ASSLING                320
  ARGENT    RON ARGENT                   1165
  GRAAFF    PAUL DE GRAAFF                 35
  TANHW     HOON WEE TAN                  502
  SVFM05    SVFM STUDENT 05              3590
  SILVIO    SILVIO PODCAMENI              763
  ALVAREZ   RICARDO ALVAREZ                44
  ERICH     ERIC HANSEN                    38
  HILDING   HILDING LANDEN                 59
```

Figure 29. OpenEdition User-Related Information

Show RRSF User Information (System Wide): The report shows the status of defined password synchronization profiles in the various systems. It also shows whether there are any pending associations either locally or remotely. You have to keep in mind that all the reports describe that point in time when the RACF

database was copied. Before you take any action, you will have to verify that the situation still exists by issuing RACF commands in real time.

```
                    RACF REMOTE SHARING INFORMATION
                    ===============================

         TARGET    TARGET   CREATOR    DATE        TIME     P  R  L  P
USERID    NODE     USERID     ID      DEFINED     DEFINED   E  P  P  S
-------  --------  -------- --------  ----------  --------  -  -  -  -
ROBBYM   WTSCPLX1  KINGMA   KINGMA    01/29/1996  10:35 PM  Y  N  N  N
ROBBY2   SC47      NDRA     ROBBY2    08/25/1995  08:08 PM  Y  N  N  N
NDRA     SC47      NDRA2    NDRA      08/29/1995  07:40 PM  N  Y  N  Y
CRAIGJ   WTSCPLX1  ROBBYM   CRAIGJ    01/26/1996  09:38 PM  Y  N  N  Y
SARDELA  WTSCICF   ROBBYM   SARDELA   08/25/1995  01:54 PM  N  N  N  N
SARDELL  SC47      SARDELA  SARDELL   09/01/1995  01:55 PM  Y  N  N  Y
SARDELL  SC52      SARDELA  SARDELL   09/01/1995  01:57 PM  Y  N  N  N
MEUDT    SC47TS    SARDELL  MEUDT     08/21/1995  07:57 PM  Y  Y  N  N

  PE=PEER USERID         RP=RACF REMOTE ASSOCIATION PENDING
  S=PW SYNCH DEFINED     LP=RACF LOCAL ASSOCIATION PENDING
```

Figure 30. General RACF Remote Sharing Facility User Information

4.2.2 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 31. 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. After entering 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.

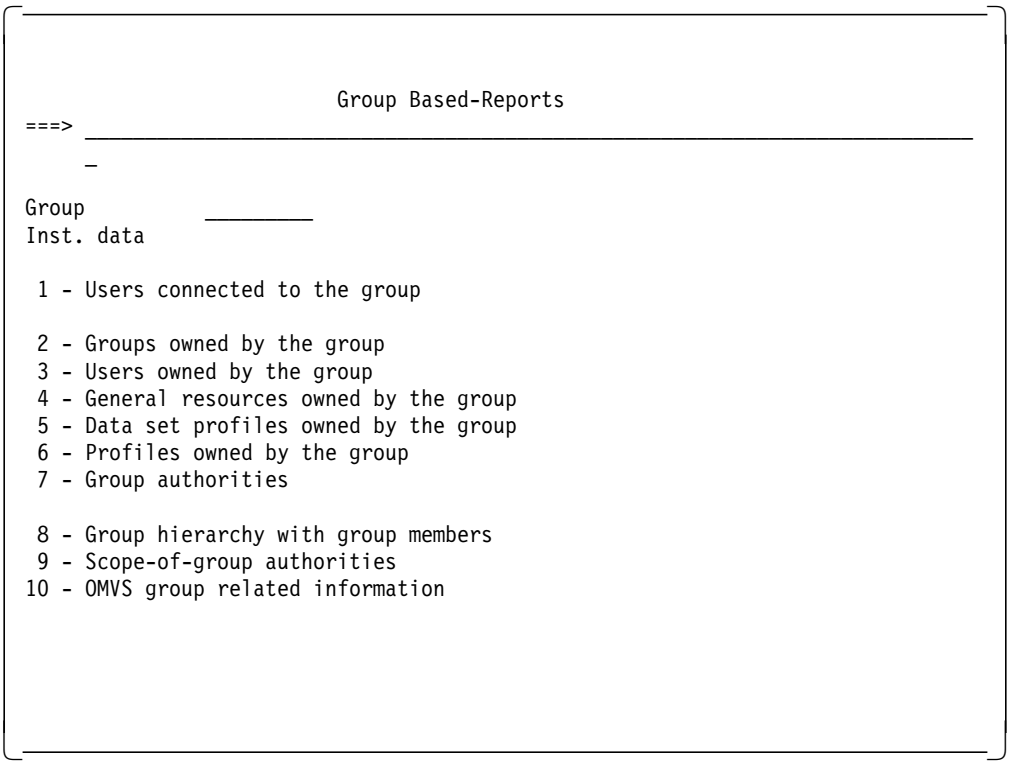


Figure 31. RACFRY01 Group-Based Reports Panel

Your chosen group will now show up on the panel from which you started, along with the information from the installation data field, where used. You can now choose 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 in what you can do with your reports. BROWSE lets you use FIND commands and scroll up, down, and sideways; a 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 in which 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 manager 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.

```
USERS OF THE GROUP: SYS1

USERID    USER NAME
--------  -----------------
ALLMOND   ALLMOND
ARCURI    ARCURI
HILDING   HILDING LANDEN
ALVAREZ   RICARDO ALVAREZ
GRAAFF    PAUL DE GRAAFF
AYRESR    ROB AYRES
BASSI     VALERIANO BASSI
```

Figure 32. User Connected to a Specific Group

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 a 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 are 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.

```
GENERAL RESOURCES OWNED BY SYS1

CLASS
NAME      UACC      RESOURCE NAME
--------  --------  -----------------
DASDVOL   READ      MXXE83
PROGRAM   NONE      ICHDSM00
PROGRAM   NONE      ICHMIN00
FACILITY  NONE      BPX.SERVER
FACILITY  NONE      DCERO05.ENTITY
PROGRAM   NONE      SU
SURROGAT  NONE      BPX.SRV.DCERO5C
STARTED   NONE      FTPSERVE.*
STARTED   NONE      IKJTEST1.*
STARTED   NONE      INETD.*
```

Figure 33. General Resources Owned by the Group

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 want to know the actual data sets that are protected by these profiles, you 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.

```
RACF PROFILES OWNED BY SYS1


 RESOURCE
  CLASS    UACC      RESOURCE NAME
+--------++--------++---------------
 DATASET   READ      SYS1.KT210.MSG
 DATASET   NONE      SYS1.UADS
 DATASET   ALTER     TPNS.*.**
 DATASET   ALTER     TPNS4.*.**
 DATASET   ALTER     VSAPL.*.**
 DATASET   ALTER     VSPASCAL.*.**
 FACILITY  NONE      BPX.SERVER
 FACILITY  NONE      DCER005.ENTITY
 GROUP     NONE      @PL
 GROUP     NONE      ACFNCP
```

Figure 34. Profiles Owned by the Group

Group Authorities: The group authorities report all of the RACF profiles that have 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 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," which shows you the groups owned by the selected group. In this report you list 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 when 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.

```
SYS1 WITH SUBGROUPS AND USERS CONNECTED TO THEM

                                                    S         G
                                                  S S -     G G -
                                                S - - A   G - - A
                                                - S O U   - S O U
                                 LAST           R P P D   R P P D
                                ACCESS          E E E I   E E E I
USERID    PROGRAMMER NAME        DATE           V C R T   V C R T
--------++--------------------++----------++-+-+-+-++-+-+-+-+
ARCHUSR2  DSM - ARCHIVAL        11/09/1994  N N N N   N N N N
ARCURI    ARCURI                07/06/1994  N N Y N   N N N N
ARGENT    RON ARGENT            -           N Y Y N   N N N N
ALVAREZ   RICARDO ALVAREZ       08/30/1995  N Y Y N   N N N N
AYRESR    ROB AYRES             -           N Y Y N   N N N N
BASSI     VALERIANO BASSI       -           N Y Y N   N N N N
HILDING   HILDING LANDEN        -           N N N N   N N N N
GRAAFF    PAUL DE GRAFF         -           N Y Y N   N N N N
```

Figure 35. Group Hierarchy with Group Members

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, 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 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.

```
RESOURCE PROFILES OWNED BY SYS1 OR ITS SUBGROUPS

CLASS
NAME      PROFILE NAME                                UACC      OWNER
--------  ------------------------------------------  --------  ------
$DCERACF  ADMINISTRATOR                               ALTER     ERICFI
$DCERACF  SC60.CURRENT                                ALTER     ERICFI
$DCERACF  SC60.V003                                   ALTER     ERICFI
$DCERACF  SC60.V004                                   ALTER     ERICFI
$DCERACF  SC60.V005                                   ALTER     ERICFI
$DCERACF  00000417-7c19-2f0b-9b00-10005ac95217        ALTER     ERICFI
ACCTNUM   ACCNT#                                      ALTER     IBMUSE
ACCTNUM   ACCT#                                       ALTER     DODELL
APPCLU    USIBMSC.SCDSCICS.SCDSCICS                   ALTER     OCONNO
APPCLU    USIBMSC.SCDSCICS.SCW1000I                   ALTER     OCONNO
```

Figure 36. Scope of Group Authorities

OMVS Group-Related Information: This report shows the relationship between RACF Group Names and the Open Edition Group ID.

Make sure that you have not specified the same Group ID for several RACF groups which could lead to unclear access rights.

```
OMVS-GROUPID / RACF-GROUP-NAME RELATED INFORMATION
==================================================

  RACF            OMVS
  GROUP           GROUP
  NAME             ID
  --------  -----------
  SYS1               0
  OMVSGRP            1
  DCEGRP             2
  TCPIPGRP           2
  TSO                4
  OP2                5
  RACFTEST           5
  OMVS             101
  TTY              200
  IMWEB            205
```

Figure 37. OpenEdition Group-Related Information

4.2.3 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.

```
REPORT BASED ON THE UNIVERSAL ACCESS OF THE RESOURCE

CLASS
NAME      UACC      OWNER     RESOURCE NAME
--------  --------  --------  ----------------------------------
DATASET   ALTER     DODELL    HSM.BACK.T000422.POLAND.ISPF.I0194
DATASET   ALTER     DODELL    HSM.BACK.T004714.P9113.S#.I0110
DATASET   ALTER     DODELL    HSM.BACK.T011914.PIERRE.ITSC.I0117
DATASET   ALTER     DODELL    HSM.BACK.T020422.PETERSE.TSCF.I0180
DATASET   ALTER     DODELL    HSM.BACK.T034614.P9112KP.GUIDE.I0110
DATASET   ALTER     DODELL    HSM.BACK.T050422.PETERSE.MISC.I0180
DATASET   ALTER     DODELL    HSM.BACK.T054314.MICHEL.VERNON.I0110
DATASET   ALTER     DODELL    HSM.BACK.T054614.P9113.MANUALS.I0110
DATASET   ALTER     DODELL    HSM.BACK.T063714.FRANCK.MASTER.I0110
```

Figure 38. Profile Based on UACC

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 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 database.

Profile reports are handy when 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 are looking for.

```
DATASET     SYS1.KT210.LOAD              READ        SYS1
DATASET     SYS1.LINKLIB                 READ        SYS1
DCEUUIDS    05145C00-C0EE-1C8F-A         NONE        BOCHE
DCEUUIDS    05145C00-C0EE-1C8F-A         NONE        MICHEL
DCEUUIDS    05145C00-C0EE-1C8F-A         NONE        HILDING
DSNR        DB3A.*                       NONE        FINNTC
FACILITY    DCER003.ENTITY               NONE        ALVAREZ
FACILITY    IRRDPI00                     NONE        DODELL
PTKTDATA    MVSESA1                      NONE        SILVIO2
PTKTDATA    MVS3090                      NONE        GRAAFF
RRSFDATA    AUTODIRECT.WTSCPLX1.         NONE        CRAIGJ
RRSFDATA    RACLINK.DEFINE.ICF           NONE        ROBBYM
```

Figure 39. Profile Information

4.2.4 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* because they show as much relevant information about each resource profile as can fit 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 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 it is really a translation of whatever has been specified in a RDEFINE command for SECDATA SECLEVEL.

The obvious fast check to make 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 your policy).

```
COMPRESSED GENERAL RESOURCE REPORT

DCEUUIDS  05145C00-C0EE-1C8F-AADD-00008C2EC0  JSTOLT    NONE      N
DCEUUIDS  05145C00-C0EE-1C8F-AADD-00008C2EC0  BOCHE     NONE      N
DSNR      DB3A.*                              FINNTC    NONE      Y
FACILITY  $RACF.GROUP.REFRESH                 FINNTC    NONE      N
FACILITY  APPCMVS.DBTOKEN                     MEUDT     NONE      Y
FIELD     USER.OMVS.UID                       ECKHARD   NONE      N
GCICSTRN  CAT1TRNS                            CICS330   NONE      N
PTKTDATA  TSOESA1                             DODELL    NONE      N
RRSFDATA  AUTODIRECT.WTSCPLX1.USER.*          CRAIGJ    NONE      N
SECLABEL  SYSNONE                             IBMUSER   NONE      N
STARTED   ANTMAIN.**                          ROBBYM    NONE      N
TSOPROC   TSOPDF                              DODELL    NONE      N
VTAMAPPL  *                                   SARDELL   NONE      Y
VTAMAPPL  APPCOMVS                            SLEKKA    NONE      N
```

Figure 40. Compressed General Resource Report

Compressed User Profile Report: This report is designed to take just a few important fields from every user profile and 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 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 USER PROFILE REPORT

                                DEFAULT   ACCESS      ACCESS    REVOKE
USERID    PROGRAMMER NAME        GROUP     DATE        TIME      DATE
--------  --------------------  --------  ----------  --------  -------
HILDING   HILDING LANDEN        SYS1      26.01.1996  13.31.58  -
ANTTI     ANTTI                 SYS1      02.12.1994  16.10.13  -
APPCSTC   MEUDT                 SYS1      16.08.1996  06.47.41  -
APPROV    ####################  DSMMVS    19.12.1995  15.33.59  -
ARCHUSR1  DSM - ARCHIVAL        SYS1      09.11.1994  10.59.09  -
GRAAFF    PAUL DE GRAAFF        SYS1      09.11.1994  10.59.10  -
ARCURI    ARCURI                SYS1      06.07.1994  17.11.35  -
ARGENT    RON ARGENT            SYS1      -           -         -
ALVAREZ   RICARDO ALVAREZ       DSMMVS    -           -         -
```

Figure 41. Compressed User Profiles Report

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 subgroups, if there are any. The group report is 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 to change that structure by 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 a numeric value, 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, for example, 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.

Compressed OMVS Profile Report: When you use RACF commands to define users and groups, the information RACF gathers from these commands is stored in profiles and placed in the RACF database.

The user profile describes an individual user or a system task. Those users who should be allowed to use the OpenEdition functions need an OMVS segment for their user profile where to specify information specific to OpenEdition. When you define a new OpenEdition MVS user or change the attributes for an existing user, you can specify the following information in the OMVS segment for the user profile:

```
HOME      User's OpenEdition MVS initial directory path name
PROGRAM   User's OpenEdition MVS initial program path name, normally the
          shell program
UID       User's OpenEdition MVS user identifier
```

Use the OMVS segment of the group profile to specify information about the group's OpenEdition MVS group ID. For example, you can use it when you define a new OpenEdition MVS group or change the OMVS attributes for an existing group. Users with a valid OMVS segment in their user profile and whose default or current connect group has an OpenEdition MVS group identifier (GID) specified can use OpenEdition MVS functions and can access OpenEdition (HFS) files based on the GID and UID values assigned.

This report shows the information for each RACF defined user detailing USERID, Default Group and User Name, related to the corresponding information for that user in the OpenEdition environment including OMVS UID, OMVS Group ID, OMVS Path, and OMVS Program.

Make sure that users have a personal UID so that you are able to ensure individual accountability even in the OpenEdition environment (excluding super users).

```
PROFILE INFORMATION FOR OPENEDITION USERS
=========================================

                                                                    OMVS
RACF     GROUP     USER                OMVS    OMVS   HOME         DEFAULT
USERID    NAME      NAME                UID     GID   PATH         PROGRAM
--------  --------  ---------------   ------  ------  -----------  ---------
ARGENT    SYS1      RON ARGENT            20       0  /u/argent    /bin/sh
ASSLING   SYS2      RAINER ASSLING       356       3  /u/assling   /bin/sh
AYRESR    SYS1      ROB AYRES            888       0  /u/ayresr    /bin/sh
BASSI     SYS3      VALERIANO BASSI       39       5  /u/bassi     /bin/sh
BENNO     SYS1      BENNO ALADJEM          4       0  /            /bin/sh
BHEU      PROD      BRIAN HEU           1234      56  /u/bheu      /bin/sh
CELIO     SYS1      CELIO COSTA          329       0  /u/celio     /bin/sh
CHENS     MARK      SCOTT CHEN            45      14  /u/chens     /bin/sh
CICSRSA   SYS1      CICSRSA               66       0  /            /bin/sh
CICSRS4   SYS1      CICS RESIDENT          7       0  /            /bin/sh
```

Figure 42. Compressed OpenEdition Profile Report

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 of 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. It shows 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 a fast search of groups of interest and to find information.

Users and Their Connect Groups: This report is a bit different from the other summary reports in that you have a multiple line output format for every user. A sample report is shown in Figure 43 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 43. Sample Users and Their Connect Groups Report

The first line shows the user ID, 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, and showing the REVOKE, AUDITOR, SPECIAL, and OPERATIONS attributes as shown 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.

All Occurrences of a User ID or Group Name: Figure 44 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 44. 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 (Page 1 of 2). 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	-

Table 1 (Page 2 of 2). Interpreting the Option 11 Report		
WHERE FOUND	**RESOURCE NAME / INSTALLATION DATA**	**CLASS/GROUP/USER**
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

4.3 Audit Reports

The *audit reports main panel* for the Audit and Report Application is shown in Figure 45. You reach this panel by selecting **A - Audit reports** from the *auditing application base panel* shown in Figure 19 on page 29.

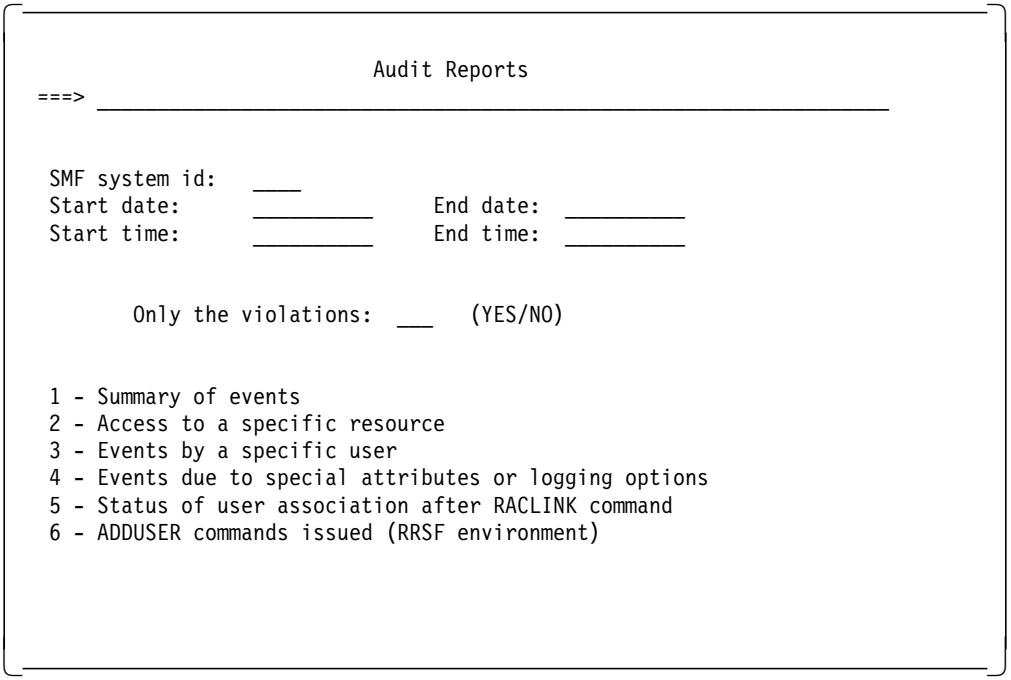


Figure 45. Audit Reports Main Panel

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 Audit and Report Application, you have to remember that QMF is used as a query manager. The percent sign (%) is used as a generic (sometimes referred to as a “wild card”) character instead of 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). For example, if you specify SYS1, the application will expand it into SYS1%. In other words, all the names you specify will be considered generic.

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 a system ID, a date window, and a time window.

System: If SMF records are written by more than one system, you can select 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* or you can ask your systems programmer.

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.

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 reports for 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.

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 46.

```
                        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 46. Event Summary Report

All events of a given type, the event qualifiers and 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. *RACF Macros and Interfaces* lists all event types and possible event qualifiers.

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

By entering an **S** in the selection column (Sel), you 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 47.

EVENT TYPE	EVENT QUAL	TERM	EVT USER ID	DATE WRITTEN	TIME WRITTEN	RES 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 47. Detailed Event List

By entering a **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.

The two rightmost columns of the summary report have a heading of “Resource name / Path name” and “New resource name / Path name / File name” respectively. Since the same form is used for many different event types, the headings do not always make sense, nor is there always data in these columns. This is because some event types reveal that an event took place but there is no meaningful data to display (JOBINIT is a typical example). For OpenEdition resources, the names shown are the path name and the file name; for file rename operations you see the new path name. There are still many OpenEdition event types where we have not specifically tailored the reports to show a resource name because you would first have to decide what information would be meaningful to audit.

Basically what you have available is a kind of skeleton from which you can mold your own favorite report.

A sample list is shown in Figure 48.

```
                        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 48. RACF Auditor Resource Report

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 find all violations against a specific resource and 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 49, 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 49. 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 50.

```
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 50. Access to Specific Resources

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 to the panel shown in Figure 51, where you can specify a user ID.

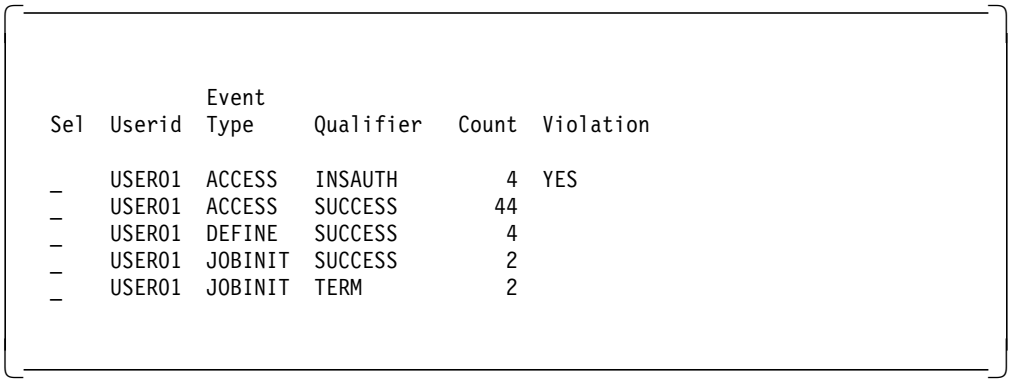
```
          Audit Reports - User ID Selection
===> ____________________________________________________________


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


      Only the violations:  ___   (YES/NO)


 User ID:  ________
```

Figure 51. User Selection Panel

Figure 52 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 whether 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.

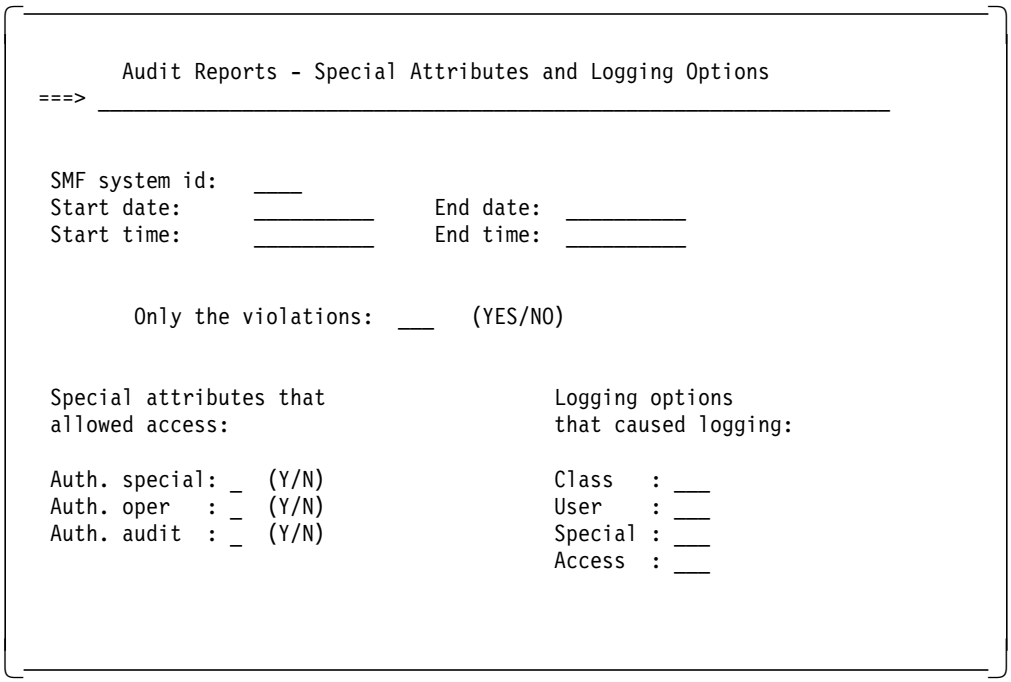
To get more detailed information, you can use this report for further processing. Typing an **S** in the selection column (SEL) will get you a detailed list with more information, including the resource name and the date and time the event occurred.



```
              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 52. Specific User Report

Events Because of Special Attributes or Logging Options: Specifying option **4 - Events due to the special attributes or logging option** on the audit reports main panel takes you to a panel shown in Figure 53, 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 53. 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 tells what events to include in the resulting report. If you make no selections at all, a report of all events is 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 54.

```
                 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 54. Events Due to SPECIAL Attribute Report

The report shows the event type, the event qualifier, the user ID, and the date and 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; an ″N″ says logging was set to off.

4.3.1 RACF Remote Sharing Information (RRSF)

The RACF Remote Sharing Facility can be used to synchronize multiple RACF databases within the same installation. The support can also be used to administer the databases from one central site without having to log on to every separate system.

RRSF is set up in cooperation with the systems programmers and is managed by definitions in RACF parameter library members and profiles in the RACF database. RRSF requires an LU 6.2 connection between the hosts that are participating in the database sharing.

Status of User Association after RACLINK Command: The RACLINK command allows you to define, approve, and delete an established or pending user ID connection, list information related to a user ID association, and establish password synchronization between user IDs. The output report lists user ID associations between users in the RRSF environment with the status and type of associations. To assist you in your security administration and auditing tasks, you can use this option to produce a report based on the output from the SMF Data Unload Utility to check these commands.

ADDUSER Commands issued (RRSF Environment): Command Direction and Automatic Command Direction can be used to perform security administration for multiple data centers from a central site without submitting batch jobs or logging on to the remote systems. ADDUSER, among other RACF TSO commands, can be directed to a local or remote node within an RRSF network. This report shows the ADDUSER commands issued from a submitting node (pointed to by ORIGINATED_FROM words) used to create the user ID (heading USERID ADDED). The issuing user ID is specified in the CMD USERID column. This report provides you with information about users who have tried to issue ADDUSER commands through Command Direction or Automatic Command Direction without authorization. For all other ADDUSER commands (non-RRSF), the COMMAND SOURCE column will be blank.

```
     ADDUSER COMMAND
     ===============

EVENT    EVENT    EVENT  JOB   USER
TYPE     QUALIF   USERID NAME   ID      CMDSRC
-------- -------  ------ ----- -------  ----------------------------------
ADDUSER  SUCCESS  HAIMO  RACF  ASSLING  ORIGINATED_FROM(WTSCPLX1.HAIMO,DIR..
ADDUSER  SUCCESS  HAIMO  RACF  FRANK    ORIGINATED_FROM(WTSCPLX1.HAIMO,DIR..
ADDUSER  SUCCESS  HAIMO  RACF  OSCAR    ORIGINATED_FROM(WTSCPLX1.HAIMO,DIR..
ADDUSER  SUCCESS  HAIMO  RACF  JDMETZG  ORIGINATED_FROM(WTSCPLX1.HAIMO,DIR..
ADDUSER  SUCCESS  HAIMO  RACF  JGREBLO  ORIGINATED_FROM(WTSCPLX1.HAIMO,DIR..
ADDUSER  SUCCESS  HAIMO  RACF  ICKIM    ORIGINATED_FROM(WTSCPLX1.HAIMO,DIR..
ADDUSER  SUCCESS  HAIMO  RACF  VALLANC  ORIGINATED_FROM(WTSCPLX1.HAIMO,DIR..
ADDUSER  SUCCESS  HAIMO  RACF  SDTEST1  ORIGINATED_FROM(WTSCPLX1.HAIMO,DIR..
ADDUSER  SUCCESS  HAIMO  RACF  SDTEST2  ORIGINATED_FROM(WTSCPLX1.HAIMO,DIR..
ADDUSER  SUCCESS  HAIMO  RACF  SDTEST3  ORIGINATED_FROM(WTSCPLX1.HAIMO,DIR..
```

Figure 55. ADDUSER Command (RRSF Environment)

4.4 Auditing and Reporting Enterprise-Wide

The Auditing and Reporting Tool focuses primarily on data, whether RACF or SMF, from one system. It is possible to load data from multiple OS/390 systems into the DB2 tables. To separate the data loaded will not pose a problem for the SMF-related data, because there is an SMF-ID in each record produced. It will pose a problem for the RACF data. There is no SMF-ID or any other indication from which system the unloaded data originated. There is nothing in the RACF database that relates it to a given OS/390 system.

Suppose we would like to share the RACF database between multiple systems, which SMF-ID would be the right one to choose? This issue might find a solution in the future, but right now it is an obstacle for enterprise wide reporting.

In Appendix C, “Sample REXX Procedure to Add SMF-ID” on page 101, a sample REXX procedure is supplied which stores one character into the fifth position of every record. This position is currently unused.

This means that all DB2 tables that are related to the RACF unload utility (IRRDBU00), should have an additional field defined to account for the SMF-id of the system. It also means that new indexes should be created including the SMF-ID field. Some of the indexes used today are unique and do not allow for duplicate entries. So you would need to create the indexes with the SMF-ID field included to separate the data from multiple RACF databases.

To get the true SMF-ID into the DB2 tables, the single character that was loaded into them needs to be translated to reflect the actual SMF-ID. This can be achieved through a simple query, which updates all SMF-ID fields when they are equal to a given character, for example :

```
-------------------------------------------------------------
--   SET ALL RECORDS TO SMF-ID 3090 WHEN THE LOADED FIELD IS 1
-------------------------------------------------------------
UPDATE  HILDING.GROUP_BD
     SET GPBD_SMF_ID = '3090'
     WHERE GPBD_SMF_ID = '1'
```

This two-step process is a bit cumbersome, but currently there is no other way of achieving this.

Be aware that if you choose this approach, you will also have to change the reporting part of the application to include the SMF-ID.

4.5 Auditing the Internet Connection Server for OS/390

Our report application does not specifically address auditing of the Internet Connection Server for OS/390, but there are reports like the “Summary of events” (see “Summary of Events” on page 54) that will show events emanating from the Internet Connection Server. Whether you will see such events or not will depend on the audit options that you have specified in RACF as well as what logging is done in the Internet Connection Server.

The event type ′FACCESS′ (file access in OpenEdition) will be logged for your GET and POST requests in the Internet Connection Server. However, mostly the requests are done by a surrogate user such as PUBLIC and the real user behind the request is not known to RACF. The Internet Connection Server keeps its own logs for both errors and access requests where you can see the remote host name (or IP address, or DNS host name), the name of the authenticated user (if that was required), the date and time, and the request as entered. However, you cannot directly correlate the request as entered from the browser and the file accessed according to the report from SMF. The basic reason for this is that the Internet Connection Server does have a configuration file that quite often results in the conversion of the path name of the incoming request into something else. Looking at the Internet Connection Server log file and the SMF records for file access, we found that you can relate the date, time and file name (the part beyond the last ′/′ in the path name).

You may wonder why a correlation of the Internet Connection Server log and the file accesses reported by OpenEdition might be interesting. The answer is that you could be able to identify the actual user that did the request, or at least be

able to identify the host from where it originated. Again that may not be all that easy. As you may know, there are ways of “spoofing” your IP address (that is, you modify it to someone else′s) and if you are using a firewall, all you are seeing is the address of the firewall.

Looking at all these facts, it may not be all that interesting to go through the work of creating yet another table and some additional queries just to find some additional information that is of limited use and not necessarily to be trusted. Of course you may want to do it on occasion anyway, if you suspect someone is trying to misuse information or penetrate your installation.

4.6 QMF Hints and Tips

Most of the queries that are used to build the reports in the Audit and Report Application are simple SQL queries. However, to create reports, you sometimes need to make decisions and pass information from one query to another. It is for this function that QMF was chosen since it has a REXX interface that can be used in building reports that require iterative queries and logic. As mentioned earlier, you need at least QMF Version 3 Release 1.1, since this is the first release with the REXX interface.

4.6.1 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 then 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. Creating these kinds of views is not an easy task, however, since there is no single field in every table that would be a logical way to define a limitation of rights. Because of the nature of the contents of the DB2 databases built from the RACF Database Unload Utility and the RACF SMF Data Unload Utility, you must protect them as you protect the RACF database and the SMF database, respectively. Make sure that the databases are not granted to the public and also make sure that the SYSADM authority is limited to only a few people.

4.6.2 Modifying QMF Reports and Queries

The *auditing application base panel* option **Q** for the Query Management Facility 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 shown again, but now you can change the FORM, or the QUERY, or both, and produce a report that is more to your liking.

If you have chosen QMF as your report browsing option (see Figure 18 on page 26), then you do not have to return to the base panel in order to change the FORM or the QUERY; you only need to use the PF keys as shown on your screen.

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 straightforward.

You can write your SAVE command in the format “SAVE FORM AS ?,” after which 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 do not specify the share option as “yes,” then only you can use that particular FORM or QUERY.

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 (so scrolling is necessary).

```
IBM*     Licensed Materials - Property of IBM
5706-254 5706-255 (c) Copyright IBM Corp. 1982, 1992.
US Government Users Restricted Rights - Use, duplication
disclosure restricted by GSA ADP Schedule Contract with IBM
* Trademark of International Business Machines Corp.

 QMF HOME PANEL
 Version 3 Release 1.1          *******    **    **      *****
                               **     **   ***   ***     **
 Query                        **     **   ****  ****    *****
 Management                   **     **   ** ** ** **   **
 Facility                    **   * **   **  ****  **  **
                              ******    **   **    ** **
 Connected to                      *
 WTSCICF

Type command on command line or use PF keys.For help,press PF1

1=Help      2=List        3=End     4=Show   5=Chart     6=Query
7=Retrieve  8=Edit Table  9=Form   10=Proc  11=Profile  12=Report
OK, you may enter a command.
COMMAND ===>
```

Figure 56. QMF Main Panel

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. Or you can simply press the PF key for FORM (normally PF9).

Using the same logic you may also change, for instance, 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 (by changing the ORDER BY), and run the query again with your new sort order. The changes you make are only temporary until you enter a SAVE command.

Note that the report application comes with a naming convention for naming objects (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.

4.7 Modifying the Auditing Package

The Audit and Report 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 4.6, “QMF Hints and Tips,” or you may create completely new selections by adding your new functions to the base panel or any of the subpanels, or, by 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.

4.8 ISPF Hints and Tips

ISPF panels are used by the Audit and Report Application to provide the interface between the user and the report application. The panels can easily be 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 probably need to be tailored to the way your installation uses the help function. Quite often it can be helpful to provide the user with the phone number of the Help Desk or of a person to contact when necessary.

If you see a need for changing the information presented on the panels, you can always enter PANELID in the command field on your screen, which shows you the name of the current panel. Knowing this, you can modify the correct panel in the PANELS dataset.

When translating the panel text to your own language, save the originals in a separate library for later reference, if needed.

4.8.1 ISPF Help Panel Structure

The help panels have been set up so that a user can press the HELP key on the base panel and then be presented with all the options by just pressing the enter key. Users can select the particular option that they want information about by then 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, G is for the group-based reports panel and A is for the audit reports.
- The last character or characters correspond to the option number on the respective panels.

The U, G and A panels have an extra selection with an option of zero, which is used to explain how to fill in the selection fields at the top of the panel.

For example, suppose 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, read the note in section 4.3, “Audit Reports” on page 52. Other than that, you can change your help screens as you like, using the attributes that are normal for your installation.

When adding new selections to existing panels, or adding additional panels, you should make sure that you are also adding the corresponding help text. Be sure to understand the logic of how to specify help text panels and the hierarchy that they are part of by studying how the package is built. If you are a seasoned systems programmer that should be no problem; if you are less experienced there are lot of examples to learn from.

Chapter 5. Extending the Audit and Report Application to Support a Web Browser

This chapter is a discussion about possible ways of extending the use of the Audit and Report Application, mainly to support alternative ways of interfacing with DB2 information.

5.1 Introduction

As new technologies evolve, such as Internet and intranet applications, we looked at the ways by which you can extend the reach of auditing and reporting into these new environments.

Currently auditors need access to the TSO environment to be able to do some kind of auditing or reporting on the OS/390 Security Server. This may not always be possible and printed paper is still often used to supply the necessary information. From an environmental point of view we should limit the amount of paper listings that we produce.

To extend the current environment, we looked at the products currently available (or soon to be available) in an OS/390 environment. This is not to say that this kind of reporting is limited to the OS/390 environment. Corresponding products are available on other platforms as well, such as AIX or OS/2.

5.2 A Look at Where We Stand

When you run OS/390, you now have an option of running an OS/390 Web server. You can connect the OS/390 Web server to DB2 through the use of the DB2 World Wide Web Connection (DB2 WWW Connection) and start a query against your DB2 databases.

5.3 DB2 WWW Connection

The DB2 WWW Connection gives you the full power of HTML and the versatility of SQL to access data in DB2 databases (and other databases with DataJoiner) from anywhere on the Internet (or intranet) as shown in Figure 57 on page 68.

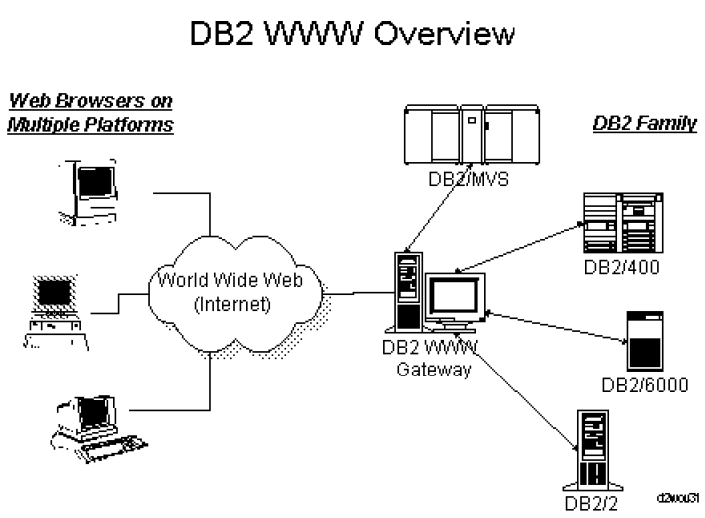


Figure 57. DB2 WWW Connection Overview

An application programmer writes macros, which are stored on the Web Server, letting anybody query databases using HTML forms. The results of the query are displayed on the Web browser. The completed macros reside on the Web Server. The development and runtime environments are illustrated in Figure 58.

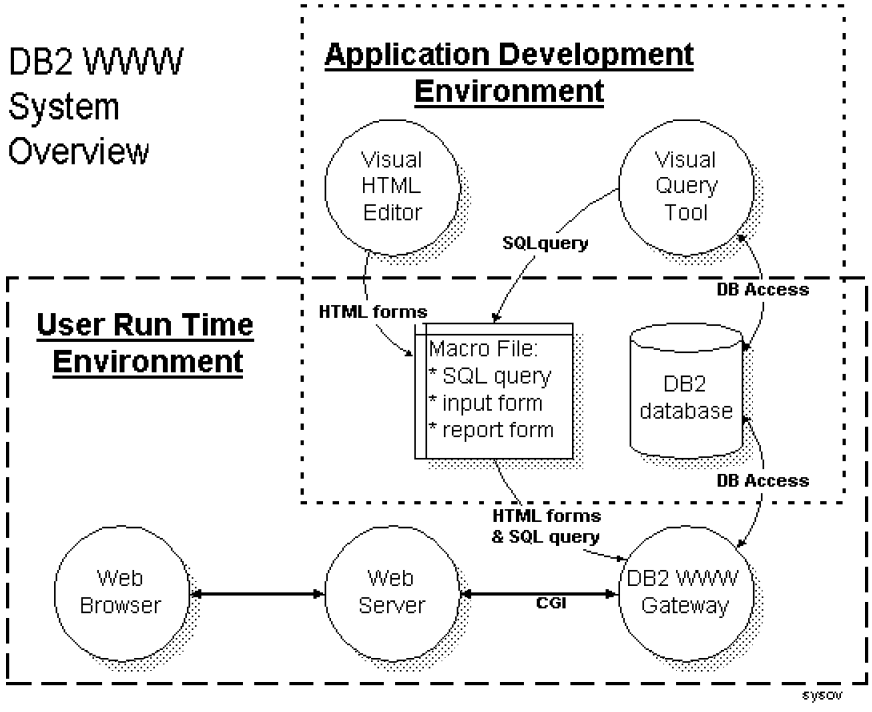


Figure 58. DB2 WWW Connection Overview

The process is transparent to people using the application because the DB2 WWW macros are invoked like any other CGI program. To run the application, they just need to submit the completed form. Figure 59 shows how the runtime flow is controlled.

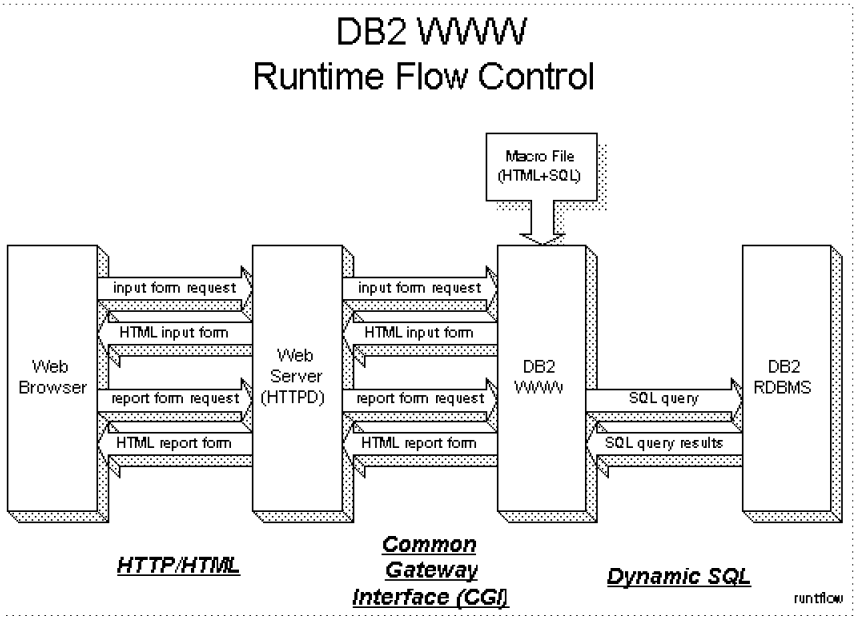


Figure 59. DB2 WWW Connection Overview

5.4 DB2 WWW Macros

A DB2 WWW macro is a file containing HTML tags and SQL statements and usually consists of four or more sections:

- A DEFINE section to define variables used in the macro
- An HTML input section to receive input from the client Web browser to be placed in the SQL query
- An SQL section to define the query to send to the database
- An HTML report section to invoke the SQL query and display the results to the client Web browser

The SQL Query is dynamically created using the variables specified in the HTML form in the SQL section. How much information people can access through the DB2 WWW depends on the security features that you have enabled on the Web server and for DB2, plus the contents of the HTML form and the SQL query.

To write a macro you only need to know HTML, SQL, and the few specifics of macro design.

5.5 DB2 WWW Security

The DB2 WWW has some security features, but they are dependent on the environment in which it is running:

- Authentication

  A DB2 WWW connection gateway supports two types of authentication:

  - Most Web servers allow you to specify which directories on the server to protect. You can also have your system require a user ID and password for people accessing files in directories of your choice. See the administrator′s guide for your Web server to determine your system′s capabilities.
  - DB2 on most platforms has an authentication mechanism for database access that can allow access to tables and columns for certain users. You can use the special variables, LOGIN and PASSWORD, in the DB2 WWW Connection to pass information into the authentication routine in DB2.

- Encryption

  You can encrypt all data sent between a client and your Web server when you use a Web server which supports the Secured Socket Layer (SSL) or the Secured Hypertext Transfer Protocol (S-HTTP). These security measures encrypt login IDs, passwords, and all data sent through HTML forms from the client and all data sent from the Web Server.

- Firewall

  The DB2 WWW Connection may be used with IBM′s Firewall and most other available firewall products, which protect both the DB2 WWW Connection server and the network from external probes or attacks.

5.6 Our Application

Our application, which uses the Web interface into DB2, does not completely emulate our TSO/ISPF-based application; we just want to show the possibilities of using a Web browser. By supplying you with the sample DB2 WWW macros that we created, as well as the related HTML pages, you should be able to tailor them to suit your own application.

5.6.1 The Home Page

The home page gives you two options to choose from:

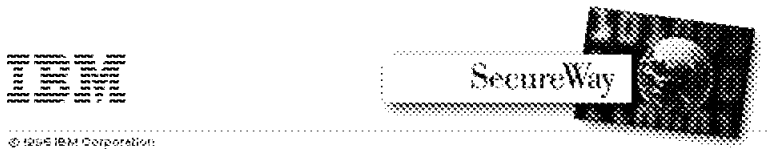
- SMF data selection

  This will give you a summary of all SMF records grouped by event_type and event_qualifier. This option resembles option A.1 in the TSO/ISPF application.

- RACF data selection

  This report primarily focuses on basic user related RACF data, and user access to RACF protected resources. The report on user access to resources resembles option 1.7 in the TSO/ISPF application.

The home page is shown is Figure 60.



Welcome to the OS/390 Security Server Audit & Reporting Tool

What report would you like to make ?

SMF data selection

RACF data selection

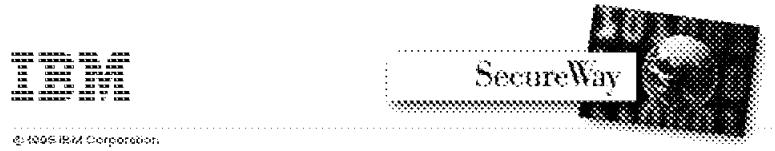
These pages were created as samples for the IBM OS/390 Security Server A.R.T.
The data and information presented are for demonstration purposes only. ©IBM Corp. 1995,1996

Figure 60. OS/390 Security Server Auditing and Reporting Tool Home Page

5.6.2 SMF Data Selection

This option will give you a summary of all SMF records grouped by event_type and event_qualifier. This option resembles option A.1 in the TSO/ISPF application.

The following page is then presented,



OS/390 Security Server Audit & Reporting Tool

Here is the list you requested :

Click on R(esource), S(elect) or U(ser) for more detail

Event Type	Event Qualifier	Count	Violation
U-S-R-DACCESS	SUCCESS	116	N
U-S-R-FACCESS	SUCCESS	1086	N
U-S-R-PERMIT	SUCCESS	4	N
U-S-R-RDEFINE	SUCCESS	4	N
U-S-R-RDELETE	SUCCESS	1	N

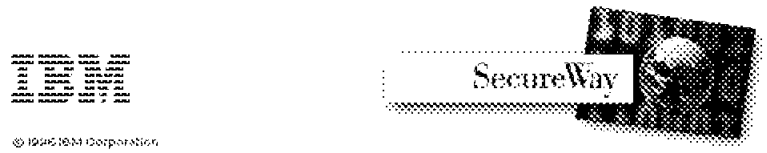
These pages were created as samples for the IBM OS/390 Security Server A.R.T
The data and information presented are for demonstration purposes only. ©IBM Corp. 1995,1996

Figure 61. SMF Data Selection Page

You are given the option of selecting more detailed information:

- U(ser)

  This option gives you a report on the Event_Type grouped by user. See Figure 62.



These are the results from the detailed query

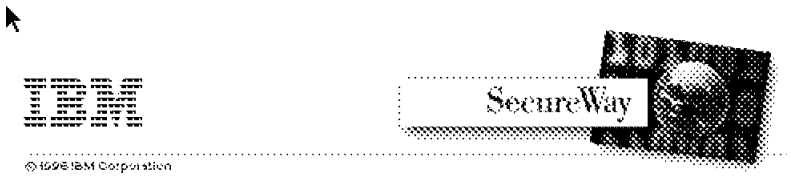
Userid	Event type	Event Qualifier	Violation	Count	Name of the user
ANTONIO	DACCESS	SUCCESS	N	16	ANTONIO
PUBLIC	DACCESS	SUCCESS	N	6	##########
RCONWAY	DACCESS	SUCCESS	N	44	RCONWAY
STC	DACCESS	SUCCESS	N	2	STARTED TASK
WEBADM	DACCESS	SUCCESS	N	10	##########
WEBSRV	DACCESS	SUCCESS	N	38	##########

These pages were created as samples for the IBM OS/390 Security Server A.R.T. The data and information presented are for demonstration purposes only. ©IBM Corp. 1995,1996

Figure 62. Detailed SMF Data Selection Grouped by User

- S(elect)

  This option gives a detailed overview of all records related to the selected Event_Type and Event_Qualifier. See Figure 63.



These are the results from the detailed query

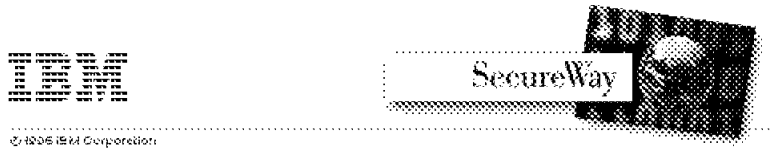
DACC_EVENT_TYPE	DACC_EVENT_QUAL	DACC_TIME_WRITTEN	DACC_DATE
DACCESS	SUCCESS	14.06.39	1996-10-08
DACCESS	SUCCESS	14.06.39	1996-10-08
DACCESS	SUCCESS	14.08.01	1996-10-08
DACCESS	SUCCESS	14.08.01	1996-10-08
DACCESS	SUCCESS	14.08.02	1996-10-08
DACCESS	SUCCESS	14.08.03	1996-10-08
DACCESS	SUCCESS	14.08.18	1996-10-08
DACCESS	SUCCESS	14.08.27	1996-10-08
DACCESS	SUCCESS	15.13.41	1996-10-08
DACCESS	SUCCESS	15.13.41	1996-10-08

These pages were created as samples for the IBM OS/390 Security Server Audit & Reporting Tool
The data and information presented are for demonstration purposes only. ©IBM Corp. 1995,1996

Figure 63. Detailed SMF Records Based on Event_Type and Event_Qualifier

- R(esource)

  This option gives a more detailed overview of the RACF resources acted upon. See Figure 64.



These are the results from the detailed query

Event Type	Event Qual	Terminal	Userid	Date	Time	Resource
PERMIT	SUCCESS	TCP00002	ANTONIO	1996-10-08	15.50.43	DFHAPPL.**
PERMIT	SUCCESS	SCT403BB	GRAAFF	1996-10-08	15.01.50	**
PERMIT	SUCCESS	SCT403BB	GRAAFF	1996-10-08	15.03.15	**
PERMIT	SUCCESS	SCT3056C	HILDING	1996-10-08	15.46.29	DFHAPPL.**

These pages were created as samples for the IBM OS/390 Security Server A.R.T. The data and information presented are for demonstration purposes only. ©IBM Corp. 1995,1996

Figure 64. Detailed Overview Related to the Event_Type and Event_Qualifier

5.6.3 RACF Data Selection

This option gives you an overview of all user IDs defined to RACF. Based on this data, it is then possible to select more detailed information. See Figure 65.

OS/390 Security Server Audit & Reporting Tool

Here is the list you requested :

Click on R(esource) or U(ser) for more detail

Userid
R- U-ADROGO
R- U-ANTOGNI
R- U-ANTONIO
R- U-ARNOLDC
R- U-BILL
R- U-BONUS2
R- U-BPXROOT
R- U-CARLINN
R- U-CATHCAM
R- U-CZUK

These pages were created as samples for the IBM OS/390 Security Server A.R.T.
The data and information presented are for demonstration purposes only. ©IBM Corp. 1995,1996

Figure 65. RACF Data Selection Page

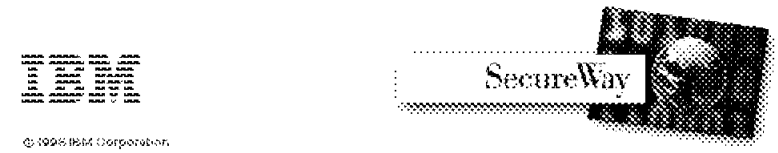
Two options are given to select more detailed information :

- R(esource)

  This option provides an overview of all RACF profiles (datasets and general resources) to which the selected user has access.

  Note: This overview does not include explicitly denied (NONE) accesses.

  See Figure 66.



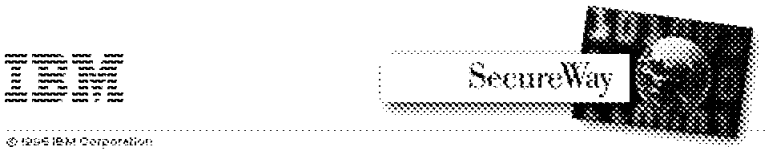
These are the results for userid ADROGO

DB2 Table	Access	Classname	Profile	Reason
DS_ACCESS	ALTER	DATASET	L123.*.**	SYS1
DS_ACCESS	ALTER	DATASET	SHARE.CONFIG.IOCDS	SYS1
DS_ACCESS	ALTER	DATASET	SYS1.*.**	SYS1
DS_ACCESS	UPDATE	DATASET	SYS1.HASPACE	SYS1
DS_ACCESS	UPDATE	DATASET	SYS1.HASPCKPT	SYS1
DS_ACCESS	UPDATE	DATASET	SYS1.KT210.LOAD	SYS1
DS_ACCESS	UPDATE	DATASET	SYS1.KT210.MSG	SYS1
DS_ACCESS	UPDATE	DATASET	SYS1.LINKLIB	SYS1
DS_ACCESS	UPDATE	DATASET	SYS1.RACFMXA	SYS1
DS_ACCESS	UPDATE	DATASET	SYS1.RACFMXAB	SYS1
DS_BD	ALTER	DATASET	@PL.*.**	UACC
DS_BD	ALTER	DATASET	ACFNCP.*.**	UACC
DS_BD	READ	DATASET	ADCLE.*.**	UACC

Figure 66. Detailed Overview of All RACF Profiles the User Has Access To

- U(ser)

  This option gives a more detailed overview of the RACF defined user. See Figure 67.



These is the detailed user record for ADROGO

Name	Creation Date	Owner	Special	Operations	Auditor	Revoke	Password interval
ADROGO	1996-09-10	TONYN	Y	Y	N	N	1996-09-10

These pages were created as samples for the IBM OS/390 Security Server A.R.T. The data and information presented are for demonstration purposes only. ©IBM Corp. 1995,1996

Figure 67. Detailed Overview of the Selected RACF User ID

5.7 Conclusion

Sample DB2 WWW macros and HTML pages are supplied in Appendix B, “Sample DB2 WWW Macros and HTML Pages” on page 83. The DB2 WWW Connection product does not allow for a full duplication of the TSO/ISPF-based application. The product is limited in function. The follow-on product, Net.Data, does allow for a full duplication of the TSO/ISPF application. The Net.Data product for OS/390 will have REXX support, which is necessary for some of the reports.

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
```

Appendix B. Sample DB2 WWW Macros and HTML Pages

This appendix will give an overview of the structure of the HTML pages and related DB2 WWW macros used in the application.

B.1 Structure of the DB2 WWW macros

The structure of the HTML pages and related DB2 WWW macros is shown to give some idea of the processing that is involved.

1. HOMEPAGE.HTML

   This page gives the end user two options to select:

   a. RACF data selection, which calls macro RACFSELECT.D2W

   b. SMF data selection, which calls macro SMFSELECT.D2W

2. RACFSELECT.D2W

   This macro will display all RACF user IDs. The example limits the output to the first 10 records selected. The report will let you select more detailed information.

   a. U option

      The U option will select more detailed information about the user. When selecting option U, the LOOKUSEL.D2W macro is called.

   b. R option

      The R option will select all profiles (dataset and general resource) the user has access to and the reason why. When selecting option R, the LOOKURES.D2W macro is called.

3. SMFSELECT.D2W

   This macro will display all SMF records grouped by event_type and event_qualifier. From here on, it is possible to further select detailed information.

   a. U option

      The U option will select all records of that specific event_type and event_qualifier grouped by user ID. When selecting option U, the LOOKUSER.D2W macro is called.

   b. R option

      The R option will select all records of that specific event_type and event_qualifier and show the related resource information. When selecting option U, the LOOKRES.D2W macro is called.

   c. S option

      The S option will select all records of that specific event_type and event_qualifier and show the complete record created. When selecting option S, the LOOKSEL.D2W macro is called.

B.2 HOMEPAGE.HTML

```
<html>
<head>
<TITLE>AUDIT Example page</TITLE>
</head>
<BODY BGCOLOR="#FFFFFF">
<BR>
<P>
<IMG SRC="mastway.gif">

<p>
<TABLE WIDTH=480 BORDER=0>
<TR VALIGN=TOP>
<TD>
</TD>
</TABLE>

<TABLE WIDTH=480 BORDER=0>
<TR VALIGN=TOP>
</TABLE><h4>Welcome to the OS/390 Security Server A.R.T.</h4>

<dt>What report would you like to make ?
<p>
<A href="/new-cgi/db2www/racf/smfselect.d2w/report">SMF Data selection</A>
<p>
<A href="/new-cgi/db2www/racf/racfselect.d2w/report">RACF data Selection</A>
<hr>
<FONT size=-1>
<CENTER>
<A href="/BonusPak2/index.htmls">
These pages were created as samples for the IBM OS/390 Security Server
A.R.T.<br>
The data and information presented are for demonstration purposes only.
&copy IBM Corp. 1995,1996</A>
</center></font>
</FORM>
</BODY>
</HTML>
```

B.3 RACFSELECT.D2W

```
<- racfselect.d2w called from the homepage ->
%define ow="GRAAFF"
%define tb="USER_BD"
%define RPT_MAX_ROWS="10"
%HTML_INPUT{
<html>
<head>
</head>
<body bgcolor="#FFFFFF">
<img src="/graaff/mastway.gif" width=380 height=105 border=0><br>
</BODY>
</HTML>
%}
%SQL {
SELECT USBD_NAME
      FROM $(ow).$(tb)
%SQL_REPORT {
<B>Here is the list you requested :</B>
<P>Click on R(esource) or U(ser) for more detail
<P>
<TABLE BORDER=1>
<TR>
<th><font size=-1>Userid</font></th>
</TR>
%ROW{
<TR>
<TD>
<font size=-1>
<A href="/new-cgi/db2www/racf/lookures.d2w/report?
    act=$(V1)">R</A>-
<A href="/new-cgi/db2www/racf/lookusel.d2w/report?
    act=$(V1)">U</A>-$(V1)</td>
</TR>
%}
</TABLE>
</CENTER>
%}
%SQL_MESSAGE {
100: "No entries found for search argument for $(name)" : continue
%}
%}
%HTML_REPORT{
<head>
<TITLE>OS/390 Security Server Audit Consultation</TITLE>
<body bgcolor="#FFFFFF">
<TABLE WIDTH=480 BORDER=0>
<TR VALIGN=TOP>
<BR>
<P>
<IMG SRC="/graaff/mastway.gif">
<TD>
</table>
<BR>OS/390 Security Server Audit & Reporting Tool
<FORM method=POST
     action="/new-cgi/db2www/racf/racfselect.d2w/report">
</FORM>
%EXEC_SQL
```

```
<hr>
<FONT size=-1>
<CENTER>
<A href="/BonusPak2/index.htmls">
These pages were created as samples for the IBM OS/390
Security Server  A.R.T.<br>
The data and information presented are for demonstration
purposes only.  &copy IBM Corp. 1995,1996</A>
</center></font>
</BODY>
</HTML>
%}
```

B.4 LOOKUSEL.D2W

```
<- lookusel.db2w called from smfselect.d2w ->
%define ow="GRAAFF"
%define tb="USER_BD"
%define RPT_MAX_ROWS="10"
%HTML_INPUT{
<html>
<head>
</head>
<body bgcolor="#FFFFFF">
<img src="/graaff/mastway.gif" width=380 height=105 border=0><br>
</BODY>
</HTML>
%}
%SQL {
SELECT USBD_NAME, USBD_PROGRAMMER, USBD_CREATE_DATE,
      USBD_OWNER_ID,USBD_SPECIAL,USBD_OPER,
      USBD_AUDITOR, USBD_REVOKE, USBD_PWD_DATE
      FROM $(ow).$(tb) WHERE USBD_NAME LIKE '%$(act)%'
%SQL_REPORT {
<TABLE BORDER=1>
<TR>
<Th><font size=-1>Userid</font></Th>
<Th><font size=-1>Name</font></Th>
<Th><font size=-1>Creation Date</font></Th>
<Th><font size=-1>Owner</font></Th>
<Th><font size=-1>Special</font></Th>
<Th><font size=-1>Operations</font></Th>
<Th><font size=-1>Auditor</font></Th>
<Th><font size=-1>Revoke</font></Th>
<Th><font size=-1>Password expire date</font></Th>
</TR>
%ROW{
<TR>
<TD><font size=-1>$(V1)</font></TD>
<TD><font size=-1>$(V2)</font></TD>
<TD><font size=-1>$(V3)</font></TD>
<TD><font size=-1>$(V4)</font></TD>
<TD><font size=-1>$(V5)</font></TD>
<TD><font size=-1>$(V6)</font></TD>
<TD><font size=-1>$(V7)</font></TD>
<TD><font size=-1>$(V8)</font></TD>
<TD><font size=-1>$(V9)</font></TD>
</TR>
%}
</TABLE>
%}
%SQL_MESSAGE {
100: "No entries found for search argument for $(name)" : continue
%}
%}
%HTML_REPORT{
<head>
<TITLE>Test results</TITLE>
<body bgcolor="#FFFFFF">
<img src="/graaff/mastway.gif" width=480 border=0><br>

<h4>These are the results from the detailed query <H4>
```

```
<FORM method=POST
     action="/new-cgi/db2www/racf/lookusel.d2w/report">
</FORM>
%EXEC_SQL
<hr>
<FONT size=-1>
<CENTER>
<A href="/BonusPak2/index.htmls">
These pages were created as samples for the IBM OS/390 Security
Server A.R.T.<br>
The data and information presented are for demonstration
purposes only.
&copy IBM Corp. 1995,1996</A>
</center></font>
</BODY>
</HTML>
%}
```

B.5 LOOKURES.D2W

```
<- lookures.d2w called from racfselect.d2w ->
%define ow="GRAAFF"
%define tb="USER_BD"
%HTML_INPUT{
<html>
<head>
</head>
<body bgcolor="#FFFFFF">
<img src="/graaff/mastway.gif" width=380 height=105 border=0><br>
</BODY>
</HTML>
%}
%SQL {
SELECT 'DS_ACCESS ' , DSACC_ACCESS, 'DATASET', DSACC_NAME,
      DSACC_AUTH_ID
      FROM $(ow).DS_ACCESS
      WHERE DSACC_AUTH_ID = '$(act)'
            OR DSACC_AUTH_ID = '*'
            AND DSACC_ACCESS <> 'NONE'
UNION
SELECT 'DS_ACCESS ' , DSACC_ACCESS, 'DATASET', DSACC_NAME,
      DSACC_AUTH_ID
      FROM $(ow).DS_ACCESS, $(ow).USER_GROUPS
      WHERE USGCON_NAME = '$(act)'
            AND DSACC_AUTH_ID = USGCON_GRP_ID
            AND DSACC_ACCESS <> 'NONE'
UNION
SELECT '*GENR_MEMBERS ' , GRMEM_GLOBAL_ACC, 'DATASET',
      SUBSTR(GRMEM_MEMBER,1,44),'GAT     '
      FROM $(ow).GENR_MEMBERS
      WHERE GRMEM_CLASS_NAME = 'GLOBAL'
            AND GRMEM_NAME = 'DATASET'
UNION
SELECT 'DS_COND_ACCESS     ' , DSCACC_ACCESS, 'DATASET',
      DSCACC_NAME, DSCACC_AUTH_ID
      FROM $(ow).DS_COND_ACCESS
      WHERE DSCACC_AUTH_ID = '$(act)'
            OR DSCACC_AUTH_ID = '*'
UNION
SELECT 'DS_COND_ACCESS     ' , DSCACC_ACCESS, 'DATASET',
      DSCACC_NAME, DSCACC_AUTH_ID
      FROM $(ow).DS_COND_ACCESS, $(ow).USER_GROUPS
      WHERE USGCON_NAME = '$(act)'
            AND DSCACC_AUTH_ID = USGCON_GRP_ID
UNION
SELECT 'GENR_ACCESS     ' , GRACC_ACCESS, GRACC_CLASS_NAME, GRACC_NAME,
      GRACC_AUTH_ID
      FROM $(ow).GENR_ACCESS
      WHERE GRACC_AUTH_ID = '$(act)'
            OR GRACC_AUTH_ID = '*'
            AND GRACC_ACCESS <> 'NONE'
UNION
SELECT 'GENR_ACCESS     ' , GRACC_ACCESS, GRACC_CLASS_NAME, GRACC_NAME,
      GRACC_AUTH_ID
      FROM $(ow).GENR_ACCESS, $(ow).USER_GROUPS
      WHERE USGCON_NAME = '$(act)'
            AND GRACC_AUTH_ID = USGCON_GRP_ID
```

```
            AND GRACC_ACCESS <> 'NONE'
UNION
SELECT 'GENR_COND_ACCESS     ' , GRCACC_ACCESS, GRCACC_CLASS_NAME, GRCACC_NAME,
      GRCACC_AUTH_ID
      FROM $(ow).GENR_COND_ACCESS
      WHERE GRCACC_AUTH_ID = '$(act)'
            OR GRCACC_AUTH_ID = '*'
UNION
SELECT 'GENR_COND_ACCESS     ' , GRCACC_ACCESS, GRCACC_CLASS_NAME, GRCACC_NAME,
      GRCACC_AUTH_ID
      FROM $(ow).GENR_COND_ACCESS, $(ow).USER_GROUPS
      WHERE USGCON_NAME = '$(act)'
            AND GRCACC_AUTH_ID = USGCON_GRP_ID
UNION
SELECT 'DS_BD     ' , DSBD_UACC, 'DATASET ', DSBD_NAME,
      'UACC '
      FROM $(ow).DS_BD
      WHERE DSBD_UACC <> 'NONE'
UNION
SELECT 'GENR_BD     ' , GRBD_UACC, 'GENERAL ', GRBD_NAME,
      'UACC '
      FROM $(ow).GENR_BD
      WHERE GRBD_UACC <> 'NONE'
      ORDER BY 1,3,4
%SQL_REPORT {
<TABLE BORDER=1>
<TR>
<Th><font size=-1>DB2 Table</font></Th>
<Th><font size=-1>Access</font></Th>
<Th><font size=-1>Classname</font></Th>
<Th><font size=-1>Profile</font></Th>
<Th><font size=-1>Reason</font></Th>
</TR>
%ROW{
<TR>
<TD><font size=-1>$(V1)</font></TD>
<TD><font size=-1>$(V2)</font></TD>
<TD><font size=-1>$(V3)</font></TD>
<TD><font size=-1>$(V4)</font></TD>
<TD><font size=-1>$(V5)</font></TD>
</TR>
%}
</TABLE>
%}
%SQL_MESSAGE {
100: "No entries found for search argument for $(name)" : continue
%}
%}
%HTML_REPORT{
<head>
<TITLE>Test results</TITLE>
<body bgcolor="#FFFFFF">
<img src="/graaff/mastway.gif" width=480 border=0><br>
<h4>These are the results from the detailed query <H4>
<FORM method=POST
     action="/new-cgi/db2www/racf/lookusel.d2w/report">
</FORM>
%EXEC_SQL
<hr>
```

```
<FONT size=-1>
<CENTER>
<A href="/BonusPak2/index.htmls">
These pages were created as samples for the IBM OS/390 Security Server A.R.T.<br
The data and information presented are for demonstration purposes only.
&copy IBM Corp. 1995,1996</A>
</center></font>
</BODY>
</HTML>
%}
```

B.6 SMFSELECT.D2W

```
%define ow="GRAAFF"
%define tb="HDR"
%define RPT_MAX_ROWS="20"
%HTML_INPUT{
<html>
<head>
</head>
<body bgcolor="#FFFFFF">
<img src="/graaff/mastway.gif" width=380 height=105 border=0><br>
</BODY>
</HTML>
%}
%SQL {
SELECT HDR_EVENT_TYPE,HDR_EVENT_QUAL,COUNT(*),MAX(HDR_VIOLATION),
      SUBSTR(HDR_EVENT_TYPE,1,4)
      FROM $(ow).$(tb)
      WHERE HDR_EVENT_TYPE IN
      ('DELRES','DELVOL','DELDSD','DELGROUP','DELUSER','PERMIT',
      'RALTER','RDEFINE','RDELETE','RVARY','APPCLU','FACCESS',
      'DACCESS','KILL','LINK','RACLINK')
      GROUP BY HDR_EVENT_TYPE, HDR_EVENT_QUAL ORDER BY 1,2
%SQL_REPORT {
<B>Here is the list you requested :</B>
<P>Click on R(esource), S(elect) or U(ser) for more detail
<P>
<TABLE BORDER=1>
<TR>
<th><font size=-1>Event Type</font></th>
<Th><font size=-1>Event Qualifier</font></Th>
<Th><font size=-1>Count</font> </Th>
<Th><font size=-1>Violation</font></Th>
</TR>
%ROW{
<TR>
<TD>
<font size=-1>
<A href="/new-cgi/db2www/racf/lookuser.d2w/report?
    act=$(V1)&act2=$(V2)&act3=$(V5)">U</A>-
<A href="/new-cgi/db2www/racf/looksel.d2w/report?
    act=$(V1)&act2=$(V2)&act3=$(V5)">S</A>-
<A href="/new-cgi/db2www/racf/lookres.d2w/report?
    act=$(V1)&act2=$(V2)&act3=$(V5)">R</A>-$(V1)</td>
<TD><font size=-1>$(V2)</font></TD>
<TD><font size=-1>$(V3)</font></TD>
<TD><font size=-1>$(V4)</font></TD>
</TR>
%}
</TABLE>
</CENTER>
%}
%SQL_MESSAGE {
100: "No entries found for search argument for $(name)" : continue
%}
%}
%HTML_REPORT{
<head>
<TITLE>OS/390 Security Server Audit & Reporting Tool Output</TITLE>
```

```
<body bgcolor="#FFFFFF">
<TABLE WIDTH=480 BORDER=0>
<TR VALIGN=TOP>
<BR>
<P>
<IMG SRC="/graaff/mastway.gif">
<TD>
</table>
<BR>OS/390 Security Server Audit & Reporting Tool
<FORM method=POST
     action="/new-cgi/db2www/racf/smfselect.d2w/report">
</FORM>
%EXEC_SQL
<hr>
<FONT size=-1>
<CENTER>
<A href="/graaff/homepage.htm">
These pages were created as samples for the IBM OS/390 Security Server A.R.T<br>
The data and information presented are for demonstration purposes only.
&copy IBM Corp. 1995,1996</A>
</center></font>
</BODY>
</HTML>
%}
```

B.7 LOOKRES.D2W

```
<- lookres.d2w called from smfselect.d2w ->
%define ow="GRAAFF"
%define tb="$(act)"
%define pre="$(act3)"
%define SHOWSQL="NO"
%HTML_INPUT{
%}
%SQL(second){
SELECT $(pre)_EVENT_TYPE,$(pre)_EVENT_QUAL,$(pre)_TERM,
       $(pre)_EVT_USER_ID,
       $(pre)_DATE_WRITTEN,$(pre)_TIME_WRITTEN, $(pre)_RES_NAME
       FROM $(ow).$(tb) WHERE $(pre)_EVENT_TYPE = '$(act)'
         AND $(pre)_EVENT_QUAL = '$(act2)'
       order by 4,5,6
%SQL_REPORT {
<TABLE BORDER=2>
<TR>
<th><font size=-1>Event Type</font></th>
<th><font size=-1>Event Qual</font></th>
<th><font size=-1>Terminal</font></th>
<th><font size=-1>Userid</font></th>
<th><font size=-1>Date</font></th>
<th><font size=-1>Time</font></th>
<th><font size=-1>Resource</font></th>
</tr>
%ROW {
<TR>
<TD><font size=-1>$(V1)</font></TD>
<TD><font size=-1>$(V2)</font></TD>
<TD><font size=-1>$(V3)</font></TD>
<TD><font size=-1>$(V4)</font></TD>
<TD><font size=-1>$(V5)</font></TD>
<TD><font size=-1>$(V6)</font></TD>
<TD><font size=-1>$(V7)</font></TD>
</TR>
%}
</TABLE>
%}
%SQL_MESSAGE {
100: "No entries found for search argument for $(name)" : continue
%}
%}
%HTML_REPORT{
<head>
<TITLE>Test results</TITLE>
<body bgcolor="#FFFFFF">
<img src="/graaff/mastway.gif" width=480 border=0><br>

<h4>These are the results from the detailed query <H4>

%EXEC_SQL(second)
<hr>
<FONT size=-1>
<CENTER>
<A href="/BonusPak2/index.htmls">
These pages were created as samples for the IBM OS/390 Security Server A.R.T.<br
The data and information presented are for demonstration purposes only.
```

```
&copy IBM Corp. 1995,1996</A>
</center></font>
</BODY>
</HTML>
%}
```

B.8 LOOKUSEL.D2W

```
<- lookusel.db2w called from smfselect.d2w ->
%define ow="GRAAFF"
%define tb="USER_BD"
%define RPT_MAX_ROWS="10"
%HTML_INPUT{
<html>
<head>
</head>
<body bgcolor="#FFFFFF">
<img src="/graaff/mastway.gif" width=380 height=105 border=0><br>
</BODY>
</HTML>
%}
%SQL {
SELECT USBD_NAME, USBD_PROGRAMMER, USBD_CREATE_DATE,
      USBD_OWNER_ID,USBD_SPECIAL,USBD_OPER,
      USBD_AUDITOR, USBD_REVOKE, USBD_PWD_DATE
      FROM $(ow).$(tb) WHERE USBD_NAME LIKE '%$(act)%'
%SQL_REPORT {
<TABLE BORDER=1>
<TR>
<Th><font size=-1>Userid</font></Th>
<Th><font size=-1>Name</font></Th>
<Th><font size=-1>Creation Date</font></Th>
<Th><font size=-1>Owner</font></Th>
<Th><font size=-1>Special</font></Th>
<Th><font size=-1>Operations</font></Th>
<Th><font size=-1>Auditor</font></Th>
<Th><font size=-1>Revoke</font></Th>
<Th><font size=-1>Password expire date</font></Th>
</TR>
%ROW{
<TR>
<TD><font size=-1>$(V1)</font></TD>
<TD><font size=-1>$(V2)</font></TD>
<TD><font size=-1>$(V3)</font></TD>
<TD><font size=-1>$(V4)</font></TD>
<TD><font size=-1>$(V5)</font></TD>
<TD><font size=-1>$(V6)</font></TD>
<TD><font size=-1>$(V7)</font></TD>
<TD><font size=-1>$(V8)</font></TD>
<TD><font size=-1>$(V9)</font></TD>
</TR>
%}
</TABLE>
%}
%SQL_MESSAGE {
100: "No entries found for search argument for $(name)" : continue
%}
%}
%HTML_REPORT{
<head>
<TITLE>Test results</TITLE>
<body bgcolor="#FFFFFF">
<img src="/graaff/mastway.gif" width=480 border=0><br>

<h4>These are the results from the detailed query <H4>
```

```
<FORM method=POST
     action="/new-cgi/db2www/racf/lookusel.d2w/report">
</FORM>
%EXEC_SQL
<hr>
<FONT size=-1>
<CENTER>
<A href="/BonusPak2/index.htmls">
These pages were created as samples for the IBM OS/390 Security
Server A.R.T.<br>
The data and information presented are for demonstration
purposes only.
&copy IBM Corp. 1995,1996</A>
</center></font>
</BODY>
</HTML>
%}
```

B.9 LOOKUSER.D2W

```
<- lookuser.d2w called from smfselect.d2w ->
%define ow="GRAAFF"
%define tb="$(act)"
%define pre="$(act3)"
%define SHOWSQL="NO"
%HTML_INPUT{
<html>
<head>
</head>
<body bgcolor="#FFFFFF">
<img src="/graaff/mastway.gif" width=380 height=105 border=0><br>
</BODY>
</HTML>
%}
%SQL(second){
SELECT $(pre)_EVT_USER_ID,$(pre)_EVENT_TYPE,$(pre)_EVENT_QUAL,
      MAX($(pre)_VIOLATION), COUNT(*), MIN($(pre)_USER_NAME)
      FROM $(ow).$(tb) WHERE $(pre)_EVENT_TYPE = '$(act)'
      AND $(pre)_EVENT_QUAL = '$(act2)'
      GROUP BY $(pre)_EVT_USER_ID, $(pre)_EVENT_TYPE,
      $(pre)_EVENT_QUAL
      order by 1,2
%SQL_REPORT {
<TABLE BORDER=1>
<TR>
<Th><font size=-1>Userid</font></Th>
<Th><font size=-1>Event type</font></Th>
<Th><font size=-1>Event Qualifier</font></Th>
<Th><font size=-1>Violation</font></Th>
<Th><font size=-1>Count</font></Th>
<Th><font size=-1>Name of the user</font></Th>
</TR>
%ROW{
<TR>
<TD><font size=-1>$(V1)</font></TD>
<TD><font size=-1>$(V2)</font></TD>
<TD><font size=-1>$(V3)</font></TD>
<TD><font size=-1>$(V4)</font></TD>
<TD><font size=-1>$(V5)</font></TD>
<TD><font size=-1>$(V6)</font></TD>
</TR>
%}
</TABLE>
%}
%SQL_MESSAGE {
100: "No entries found for search argument for $(name)" : continue
%}
%}
%HTML_REPORT{
<head>
<TITLE>Test results</TITLE>
<body bgcolor="#FFFFFF">
<img src="/graaff/mastway.gif" width=480 border=0><br>
<h4>These are the results from the detailed query <H4>
<FORM method=POST
     action="/new-cgi/db2www/racf/lookuser.d2w/report">
</FORM>
```

```
%EXEC_SQL(second)
<hr>
<FONT size=-1>
<CENTER>
<A href="/BonusPak2/index.htmls">
These pages were created as samples for the IBM OS/390 Security Server
A.R.T.<br>
The data and information presented are for demonstration purposes only.
&copy IBM Corp. 1995,1996</A>
</center></font>
</BODY>
</HTML>
%}
```

Appendix C. Sample REXX Procedure to Add SMF-ID

The following REXX procedure inserts a one-character field into the RACF database unload file to resemble an SMF-ID of the related MVS system.

C.1 ADDSYSID

```
/* REXX - Start of Specifications *********************************/
/*                                                                */
/* EXEC Name: ADDSYSID                                            */
/*                                                                */
/* Function:  Insert a single character representation of the     */
/*            SMF System ID of the system upon which this utility */
/*            executes into each of the IRRDBU00 records at       */
/*            column 5. This column is left blank by IRRDBU00.    */
/*                                                                */
/*            The character that is inserted is determined in     */
/*            the "SELECT" clause at label set_SMF_ID             */
/*                                                                */
/* Input:     The output of the RACF Data Base Unload Utility,    */
/*            allocated to DD name INDD.                          */
/*                                                                */
/* Output:    A modified version of the input data set in which   */
/*            the SMF system ID has been inserted into each record*/
/*            at column 5. This data set is allocated to DD name  */
/*            OUTDD.                                              */
/*                                                                */
/*----------------------------------------------------------------*/
/*                                                                */
/* Notice:    This sample is provided for tutorial purposes only. */
/*            It has not been submitted to any formal IBM testing */
/*            This source is distributed on an "as-is" basis,     */
/*            without any warranties either expressed or implied. */
/*                                                                */
/*            (c) Copyright 1996 IBM Corporation                  */
/*                                                                */
/* End of Specifications ******************************************/
/******************************************************************/
/*%PAGE                                                           */
/* Initializations                                                */
/******************************************************************/
OFF = 0
ON  = 1
record_count=0
address TSO
eof = 'NO'                          /* show no eof yet            */
/******************************************************************/
/* Return codes                                                   */
/******************************************************************/
good_rc=0
execio_read_error=200
execio_write_error=201
/******************************************************************/
/* - Retrieve the SMF system ID, System name, and MVS level.      */
/* - Display each of these.                                       */
/******************************************************************/
```

```
SMF_system_id=  MVSVAR('SYSSMFID')
sys_name=       MVSVAR('SYSNAME')
sys_MVS_level=  MVSVAR('SYSMVS')

say "ADDSYSID is executing on a system where:"
say "   SMF system ID="||SMF_system_id
say "   SYSNAME="||sys_name
say "   MVS="||sys_MVS_level

set_SMF_ID:
/*********************************************************************/
/* - Set the one-character value that is being inserted into the    */
/*   IRRDBU00 record at column 5. In this example, this character   */
/*   is selected based on the SMF_system_ID.                        */
/*********************************************************************/

select
   when SMF_system_ID='VMSP'  then IRRDBU00_ID='V'
   when SMF_system_ID='IM13'  then IRRDBU00_ID='I'
   when SMF_system_ID='AQTS'  then IRRDBU00_ID='A'
   otherwise                  IRRDBU00_ID='?'
   end

do until eof = 'YES'                  /* loop reading data          */
  "execio 100 diskr indd (stem IRRDBU00."
  execio_rc=rc
  select
     when execio_rc=2 then eof ='YES'
     when execio_rc=0 then nop
     otherwise do
        say "EXECIO-read has returned an unexpected return code of ",
        execio_rc
        exit(execio_read_error)
     end
  end
  do i = 1 to irrdbu00.0              /* loop through data we read  */
    record_count=record_count+1
    outrec.i=,
      overlay(IRRDBU00_ID,irrdbu00.i,5) /* Insert the system ID     */
  end                                 /* End loop through data      */
  "execio" irrdbu00.0 "diskw outdd (stem outrec."
    execio_rc=rc
    if execio_rc¬=0 then do           /* Unexpected EXECIO RC       */
       say "EXECIO-write has returned an unexpected return code of ",
            execio_rc
       exit(execio_write_error)
    end                               /* End unexpected EXECIO RC   */
end                                   /* End loop reading data      */
/*********************************************************************/
/* - Print stats                                                     */
/*********************************************************************/
Say "-------------------------------------------------------------"
Say "Summary: Processed " record_count "records."
return(good_rc)
```

Appendix D. How to Obtain the Audit and Report Application

The following procedure describes how to obtain the Audit and Report Application using the File Transfer Protocol (FTP) through the Internet.

D.1 FTP Server

The tool is stored at the Large Scale Computing FTP server in Poughkeepsie, NY, U.S.A.

The URL of the FTP server is:

ftp://lscftp.pok.ibm.com/pub/racf/mvs

1. Log in as *anonymous*
2. Password is your e-mail adress
3. Perform a "CD" to the "/pub/racf/mvs/os390art" directory
4. Change to binary mode by typing "binary"
5. The following files will be there:
   - os390art.xmit.panels

     Contains ISPF panels
   - os390art.xmit.rexx

     Contains REXX procedures
   - os390art.xmit.exp.data

     Used by QMF for loading QMF objects
   - os390art.xmit.query

     Contains QMF queries
   - os390art.xmit.proc

     Contains QMF procedures
   - os390art.xmit.form

     Contains QMF forms

After you receive these files, you can upload them to your MVS system through a file transfer program (FTP or IND$FILE).

Make sure that these are uploaded as binary files. The files should then be processed with the TSO receive command:

```
RECEIVE INDATASET(dsname)
```

This should be performed for all files.

For further installation instructions see Chapter 3, "Installing the Audit and Report Application" on page 23

Appendix E. Special Notices

This publication is intended to help OS/390 Security Server 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 OS/390 Security Server or Query Management Facility (QMF). See the PUBLICATIONS section of the IBM Programming Announcement for the OS/390 Security Server and for QMF 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.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

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 are trademarks of the International Business Machines Corporation in the United States and/or other countries:

CICS	DATABASE 2
DB2	DFSORT
Enterprise System/3090	Enterprise Systems Architecture/390
IBM	MVS/ESA
OpenEdition	OS/390
QMF	RACF

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Microsoft, Windows, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

Java and HotJava are trademarks of Sun Microsystems, Inc.

Other trademarks are trademarks of their respective companies.

Appendix F. Related Publications

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

OS/390 Security Server

- *OS/390 Security Server External Security Interface (RACROUTE) Macro Reference*, GC28-1922
- *OS/390 Security Server (RACF) Auditor's Guide*, SC28-1916
- *OS/390 Security Server (RACF) Command Language Reference*, SC28-1919
- *OS/390 Security Server (RACF) Introduction*, GC28-1912
- *OS/390 Security Server (RACF) General User's Guide*, SC28-1917
- *OS/390 Security Server (RACF) Macros and Interfaces*, SC28-1914
- *OS/390 Security Server (RACF) Messages and Codes*, SC28-1918
- *OS/390 Security Server (RACF) Planning: Installation and Migration*, GC28-1920
- *OS/390 Security Server (RACF) Security Administrator's Guide*, SC28-1915
- *OS/390 Security Server (RACF) System Programmer's Guide*, SC28-1913
- *OS/390 Security Server (RACF) (OpenEdition DCE Security Server) Overview*, GC28-1938
- *RACF Version 2 Release 2 Technical Presentation Guide*, GG24-2539
- *RACF Version 2 Release 2 Installation and Implementation Guide*, SG24-4580
- *RACF Version 2 Release 1 Installation and Implementation Guide*, GG24-4405
- *RACF Support for Open Systems Technical Presentation Guide*, GG26-2005

Query Management Facility (QMF)

- *Introducing QMF*, 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

SystemView Enterprise Performance Data Manager/MVS (EPDM)

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

REXX Publications

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

DFSORT Publication

- *DFSORT Application Programming Guide*, SC33-4035

IBM Internet Connection Secure Server

- *Up and Running*, GC31-8312
- *Webmaster's Guide*, GC31-8288
- *How to Secure the Internet Connection Server for MVS/ESA*, SG24-4803
- *Web Programming Guide*, available in HTML format from your server's Front Page or in PDF format from this URL: http://www.ics.raleigh.ibm.com

How To Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at URL http://www.redbooks.ibm.com.

How IBM Employees Can Get ITSO Redbooks

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **PUBORDER** — to order hardcopies in United States
- **GOPHER link to the Internet** - type GOPHER.WTSCPOK.ITSO.IBM.COM
- **Tools disks**

  To get LIST3820s of redbooks, type one of the following commands:

  ```
  TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
  TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
  ```

  To get lists of redbooks:

  ```
  TOOLS SENDTO WTSCPOK TOOLS REDBOOKS GET REDBOOKS CATALOG
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET LISTSERV PACKAGE
  ```

  To register for information on workshops, residencies, and redbooks:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1996
  ```

  For a list of product area specialists in the ITSO:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
  ```

- **Redbooks Home Page on the World Wide Web**

  http://w3.itso.ibm.com/redbooks

- **IBM Direct Publications Catalog on the World Wide Web**

  http://www.elink.ibmlink.ibm.com/pbl/pbl

  IBM employees may obtain LIST3820s of redbooks from this page.

- **REDBOOKS category on INEWS**
- **Online** — send orders to: USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL
- **Internet Listserver**

  With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

How Customers Can Get ITSO Redbooks

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Online Orders** (Do not send credit card information over the Internet) — send orders to:

	IBMMAIL	**Internet**
In United States:	usib6fpl at ibmmail	usib6fpl@ibmmail.com
In Canada:	caibmbkz at ibmmail	lmannix@vnet.ibm.com
Outside North America:	dkibmbsh at ibmmail	bookshop@dk.ibm.com

- **Telephone orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	(long distance charges apply)
(+45) 4810-1320 - Danish	(+45) 4810-1020 - German
(+45) 4810-1420 - Dutch	(+45) 4810-1620 - Italian
(+45) 4810-1540 - English	(+45) 4810-1270 - Norwegian
(+45) 4810-1670 - Finnish	(+45) 4810-1120 - Spanish
(+45) 4810-1220 - French	(+45) 4810-1170 - Swedish

- **Mail Orders** — send orders to:

IBM Publications	IBM Publications	IBM Direct Services
Publications Customer Support	144-4th Avenue, S.W.	Sortemosevej 21
P.O. Box 29570	Calgary, Alberta T2P 3N5	DK-3450 Allerød
Raleigh, NC 27626-0570	Canada	Denmark
USA		

- **Fax** — send orders to:

United States (toll free)	1-800-445-9269	
Canada	1-403-267-4455	
Outside North America	(+45) 48 14 2207	(long distance charge)

- **1-800-IBM-4FAX (United States)** or **(+1) 415 855 43 29 (Outside USA)** — ask for:

  Index # 4421 Abstracts of new redbooks
  Index # 4422 IBM redbooks
  Index # 4420 Redbooks for last six months

- **Direct Services** - send note to softwareshop@vnet.ibm.com
- **On the World Wide Web**

Redbooks Home Page	http://www.redbooks.ibm.com
IBM Direct Publications Catalog	http://www.elink.ibmlink.ibm.com/pbl/pbl

- **Internet Listserver**

  With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank).

IBM Redbook Order Form

Please send me the following:

Title	Order Number	Quantity

- **Please put me on the mailing list for updated versions of the IBM Redbook Catalog.**

First name Last name

Company

Address

City Postal code Country

Telephone number Telefax number VAT number

- Invoice to customer number

- Credit card number

Credit card expiration date Card issued to Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

DO NOT SEND CREDIT CARD INFORMATION OVER THE INTERNET.

Index

S

T

U

V

W

Printed in U.S.A.