

z/OS



Security Server RACF Macros and Interfaces

z/OS



Security Server RACF Macros and Interfaces

Note

Before using this information and the product it supports, be sure to read the general information under Appendix G, "Notices" on page 443.

Fourth Edition, September 2002

This is a major revision of SA22-7682-02. This edition applies to Version 1 Release 4 of z/OS (5694-A01), Version 1 Release 4 of z/OS.e (5655-G52), and all subsequent releases and modifications until otherwise indicated in new editions.

Order documents through your IBM® representative or the IBM branch office serving your locality. Documents are not stocked at the address below.

IBM welcomes your comments. A form for readers' comments may be provided at the back of this document, or you may address your comments to the following address:

International Business Machines Corporation
Department 55JA, Mail Station P384
2455 South Road
Poughkeepsie, NY 12601-5400
United States of America

FAX (United States & Canada): 1+845+432-9405

FAX (Other Countries):

Your International Access Code +1+845+432-9405

IBMLink™ (United States customers only): IBMUSM10(MHVRCFS)

Internet e-mail: mhvrcfs@us.ibm.com

World Wide Web: <http://www.ibm.com/servers/eserver/zseries/zos/webqs.html>

If you would like a reply, be sure to include your name, address, telephone number, or FAX number.

Make sure to include the following in your comment or note:

- Title and order number of this document
- Page number or topic related to your comment

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

© Copyright International Business Machines Corporation 1994, 2002. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures	ix
About this document	xi
Intended audience	xi
How to use this document	xi
Where to find more information	xii
IBM systems center publications	xiv
Other sources of information	xv
To request copies of IBM publications	xvi
Summary of Changes	xix
Chapter 1. RACF Customization Macros	1
ICHERCDE Macro	1
ICHNCONV Macro	9
ICHNCONV Coding Recommendation	9
ICHNCONV DEFINE	10
ICHNCONV SELECT	10
ICHNCONV ACTION	17
ICHNCONV END	18
ICHNCONV FINAL	18
Example of a Naming Convention Table	19
ICHRFRTB Macro	20
The RACF Router Table Supplied by IBM (ICHRFR0X)	21
Chapter 2. Panel Driver Interface	25
Invoking the Panel Driver Interface	25
Panel Mapping Table	25
The ISPLINK Call	26
Example of a RACF Panel Interface Coding Sequence	26
Chapter 3. Profile Name List Service Routine	29
Invoking the Profile Name List Service Routine	29
Format of Returned Profile Name List	30
Return Codes	30
Chapter 4. Date Conversion Routine	33
Invoking the Date Conversion Routine	33
Format of Returned Converted Date	33
Return Code	33
Chapter 5. SMF Records	35
Record Type 80: RACF Processing Record	35
Table of Event Codes and Event Code Qualifiers	42
Table of Relocate Section Variable Data	54
Table of Extended-Length Relocate Section Variable Data	60
Table of Data Type 6 Command-Related Data	67
Record Type 81: RACF Initialization Record	96
Record Type 83: RACF Processing Record for Auditing Data Sets	100
Subtype 1	101
Reformatted RACF SMF Records	104
Reformatted Process Records	104
Reformatted Status Records	109

Chapter 6. RACF SMF Data Unload Utility (IRRADU00)	113
IRRADU00 Record Format	113
The Format of the Header Portion of the Unloaded SMF Records	113
Event Codes	115
Record Extensions	119
The Format of the JOBINIT Record Extension	119
Event Qualifiers for JOBINIT (Job Initiation) Records	120
The Format of the ACCESS Record Extension	121
Event Qualifiers for ACCESS Records	123
The Format of the ADDVOL Record Extension	124
Event Qualifiers for ADDVOL (Add Volume/Change Volume) Records	125
The Format of the RENAMEDS Record Extension	125
Event Qualifiers for RENAMEDS Records	126
The Format of the DELRES Record Extension	127
Event Qualifiers for DELRES (Delete Resource) Records	128
The Format of the DELVOL Record Extension	128
Event Qualifiers for DELVOL (Delete Volume) Records	129
The Format of the DEFINE Record Extension	129
Event Qualifiers for DEFINE Resource Records	130
The Format of the ADDSD Record Extension	131
Event Qualifiers for ADDSD Commands	132
The Format of the ADDGROUP Record Extension	132
Event Qualifiers for ADDGROUP Commands	133
The Format of the ADDUSER Record Extension	134
Event Qualifiers for ADDUSER Commands	135
The Format of the ALTDSD Record Extension	135
Event Qualifiers for ALTDSD Commands	136
The Format of the ALTGROUP Record Extension	136
Event Qualifiers for ALTGROUP Commands	137
The Format of the ALTUSER Record Extension	138
Event Qualifiers for ALTUSER Commands	139
The Format of the CONNECT Record Extension	139
Event Qualifiers for CONNECT Commands	140
The Format of the DELDSD Record Extension	140
Event Qualifiers for DELDSD Commands	141
The Format of the DELGROUP Record Extension	142
Event Qualifiers for DELGROUP Commands	142
The Format of the DELUSER Record Extension	143
Event Qualifiers for DELUSER Commands	144
The Format of the PASSWORD Record Extension	144
Event Qualifiers for PASSWORD Commands	145
The Format of the PERMIT Record Extension	145
Event Qualifiers for PERMIT Commands	146
The Format of the RALTER Record Extension	146
Event Qualifiers for RALTER Commands	147
The Format of the RDEFINE Record Extension	148
Event Qualifiers for RDEFINE Commands	149
The Format of the RDELETE Record Extension	149
Event Qualifiers for RDELETE Commands	150
The Format of the REMOVE Record Extension	150
Event Qualifiers for REMOVE Commands	151
The Format of the SETROPTS Record Extension	151
Event Qualifiers for SETROPTS Commands	152
The Format of the RVARY Record Extension	153
Event Qualifiers for RVARY Commands	154
The Format of the APPCLU Record Extension	154

Event Qualifiers for APPCLU (APPC Session Establishment) Records	155
The Format of the General Event Record Extension	155
Event Qualifiers for General Events	156
The Format of the Directory Search Record Extension	156
Event Qualifiers for Directory Search Records	158
The Format of the Check Directory Access Record Extension	158
Event Qualifiers for Check Directory Access Records	160
The Format of the Check File Access Record Extension	160
Event Qualifiers for Check File Access Records	162
The Format of the Change Audit Record Extension	162
Event Qualifiers for Change Audit Records	165
The Format of the Change Directory Record Extension	165
Event Qualifiers for Change Directory Records	166
The Format of the Change File Mode Record Extension	166
Event Qualifiers for Change File Mode Records	169
The Format of the Change File Ownership Record Extension	169
Event Qualifiers for Change File Ownership Records	171
The Format of the Clear SETID Bits Record Extension	171
Event Qualifiers for Clear SETID Records	173
The Format of the EXEC SETUID/SETGID Record Extension	173
Event Qualifiers for EXEC with SETUID/SETGID Records	174
The Format of the GETPSENT Record Extension	174
Event Qualifiers for the GETPSENT Record Extension	175
The Format of the Initialize z/OS UNIX Record Extension	176
Event Qualifiers for the Initialize z/OS UNIX Record Extension	177
The Format of the z/OS UNIX Process Completion Record	177
Event Qualifiers for the z/OS UNIX Process Complete Record Extension	178
The Format of the KILL Record Extension	178
Event Qualifiers for the KILL Process Record Extension	180
The Format of the LINK Record Extension	180
Event Qualifiers for LINK Records	181
The Format of the MKDIR Record Extension	182
Event Qualifiers for MKDIR Records	184
The Format of the MKNOD Record Extension	184
Event Qualifiers for MKNOD Records	187
The Format of the Mount File System Record Extension	187
Event Qualifiers for Mount File System Records	189
The Format of the OPENFILE Record Extension	189
Event Qualifiers for OPENFILE Records	191
The Format of the PTRACE Record Extension	192
Event Qualifiers for the PTRACE Process Record Extension	193
The Format of the Rename File Record Extension	193
Event Qualifiers for Rename File Records	195
The Format of the RMDIR Record Extension	195
Event Qualifiers for RMDIR Records	196
The Format of the SETEGID (SET Effective z/OS UNIX Group Identifier (GID) Record Extension	197
Event Qualifiers for the SETEGID Record Extension	198
The Format of the SETEUID (SET Effective z/OS UNIX User Identifier (UID) Record Extension	198
Event Qualifiers for the SETEUID Record Extension	199
The Format of the SETGID Record Extension	199
Event Qualifiers for the SETGID Record Extension	201
The Format of the SETUID Record Extension	201
Event Qualifiers for the SETUID Record Extension	202
The Format of the SYMLINK Record Extension	202

Event Qualifiers for SYMLINK Records	204
The Format of the UNLINK Record Extension	204
Event Qualifiers for UNLINK Records	205
The Format of the Unmount File System Record Extension	206
Event Qualifiers for Unmount File System Records	207
The Format of the Check File Owner Record Extension	207
Event Qualifiers for Check File Owner Records	209
The Format of the Check Privilege Record Extension	209
Event Qualifiers for Check Privilege Records	210
The Format of the Open Slave TTY Record Extension	210
Event Qualifiers for Open Slave TTY Records	211
The Format of the RACLINK Command Record Extension	212
Event Qualifiers for the RACLINK Command Records	214
The Format of the IPCCHK Record Extension	214
Event Qualifiers for IPCCHK Records	215
The Format of the IPCGET Record Extension	216
Event Qualifiers for IPCGET Records	217
The Format of the IPCCTL Record Extension	218
Event Qualifiers for IPCCTL Records	220
The Format of the SETGROUP Record Extension	220
Event Qualifiers for SETGROUP Record Extension	222
The Format of the CKOWN2 Record Extension	222
Event Qualifiers for CKOWN2 Records	223
The Format of the Access Rights Record Extension	223
Event Qualifiers for Access Rights Records	225
The Format of the RACDCERT Command Record Extension	225
Event Qualifiers for the RACDCERT Command Records	226
The Format of the InitACEE Record Extension	226
Event Qualifiers for the InitACEE Records	227
The Format of the Network Authentication Service Record Extension	227
Event Qualifiers for the Network Authentication Service Records	227
The Format of the RPKIGENC Record Extension	228
Event Qualifiers for the RPKIGENC Records	229
The Format of the RPKIEXPT Record Extension	229
Event Qualifiers for the RPKIEXPT Records	230
The Format of the Policy Director Authorization Services Support Record Extension	231
Event Qualifiers for Policy Director Authorization Services Support Records	231
The Format of the RPKIREAD Record Extension	231
Event Qualifiers for the RPKIREAD Records	233
The Format of the RPKIUPDR Record Extension	233
Event Qualifiers for the RPKIUPDR Records	234
The Format of the RPKIUPDC Record Extension	234
Event Qualifiers for the RPKIUPDC Records	235
The Format of the SETFACL Record Extension	236
Event Qualifiers for SETFACL Records	237
The Format of the DELFACL Record Extension	238
Event Qualifiers for DELFACL Records	239

Chapter 7. The Format of the Unloaded SMF Type 81 Data 241

Chapter 8. The Format of the Unloaded SMF Type 81 Class Data 245

Chapter 9. The Format of the Unloaded SMF Type 83 Data 247

Chapter 10. RACF Database Unload Utility (IRRDBU00) 249

IRRDBU00 Record Types	249
The Relationships among Unloaded Database Records	250
Conversion Rules of the Database Unload Utility	258
Record Formats Produced by the Database Unload Utility	258
Chapter 11. The RACF Secured Signon PassTicket	293
Generating a PassTicket	293
Using the Service to Generate a PassTicket.	293
Incorporating the PassTicket Generator Algorithm into Your Program	294
Generating a Secured Signon Session Key	301
Using the Service to Generate a Secured Signon Session Key.	301
Incorporating the Secured Signon Session Key Generator Algorithm into Your Program	303
Chapter 12. The RACF Environment Service	307
Function	307
Requirements	307
RACF Authorization.	308
Register Usage	308
Format	308
Parameters.	308
Return and Reason Codes	310
Usage Notes	311
Related Services.	311
Appendix A. ICHEINTY, ICHETEST, and ICHEACTN Macros	313
ICHEINTY Macro	314
Return Codes from the ICHEINTY Macro.	326
ICHETEST Macro	329
ICHEACTN Macro	332
Using ICHEACTN With the DATAMAP=NEW and DATAMAP=OLD Operands	335
Examples of ICHEINTY, ICHETEST, and ICHEACTN Macro Usage	343
Appendix B. REXX RACVAR	349
Appendix C. IBM-supplied class descriptor table entries.	351
Appendix D. RACF database templates	391
Format of field definitions	391
Repeat groups on the RACF database.	392
Data field types	392
Combination fields on the RACF database	393
Determining space requirements for the profiles	393
Determining space requirements for alias index entries.	395
Group template for the RACF database	395
User template for the RACF database	397
Connect template for the RACF database	407
Data set template for the RACF database	409
General template for the RACF database.	413
Reserved templates for the RACF database.	419
Appendix E. Event Code Qualifier Descriptions	421
Event Codes and Event Code Qualifiers	421
Event 1(1): JOB INITIATION/TSO LOGON/TSO LOGOFF	421
Event 2(2): RESOURCE ACCESS	424
Event 3(3): ADDVOL/CHGVOL	427

Event 4(4): RENAME RESOURCE	427
Event 5(5): DELETE RESOURCE	429
Event 6(6): DELETE ONE VOLUME OF A MULTIVOLUME RESOURCE	429
Event 7(7): DEFINE RESOURCE	429
Event 8(8)–25(19): COMMANDS	431
Event 26(1A): APPCLU	431
Event 27(1B): GENERAL AUDITING	433
Event 28(1C)–58(3A): z/OS UNIX EVENT TYPES	433
Event 59(3B): RACLINK EVENT TYPES	436
Event 60(3C)–62(3E): z/OS UNIX XPG4 EVENT TYPES	436
Event 63(3F): z/OS UNIX SETGROUPS EVENT TYPE	436
Event 64(40): X/OPEN SINGLE UNIX SPECIFICATION EVENT TYPES	437
Event 65(41): z/OS UNIX PASSING OF ACCESS RIGHTS EVENT TYPES	437
Event 66(42)–67(43): CERTIFICATE EVENT TYPES	437
Event 68(44): GRANT OF INITIAL KERBEROS TICKET	437
Event 69(45): R_PKIServ GENCERT	437
Event 70(46): R_PKIServ EXPORT	438
Event 71(47): POLICY DIRECTOR ACCESS CONTROL DECISION	438
Event 72(48): R_PKIServ QUERY	438
Event 73(49): R_PKIServ UPDATEREQ	438
Event 74(4A): R_PKIServ UPDATECERT	438
Event 75(4B): ACCESS CONTROL LISTS SETFACL	439
Event 76(4C): ACCESS CONTROL LISTS DELFACL	439
Appendix F. Accessibility	441
Using assistive technologies	441
Keyboard navigation of the user interface.	441
Appendix G. Notices	443
Programming Interface Information	444
Trademarks.	444
RACF Glossary	447
Sequence of Entries	447
Organization of Entries	447
References	447
Selection of Terms	447
Index	465

Figures

1. Relationship among the Group Record Types	252
2. Relationship among the User Record Types (Part 1 of 2)	253
3. Relationship among the User Record Types (Part 2 of 2)	254
4. Relationship among the Data Set Record Types	255
5. Relationship among the General Resource Record Types	257
6. RACF PassTicket Generator for Secured Signon	295
7. Algorithm for RACF PassTicket Time-Coder Used for Secured Signon.	296
8. Permutation Tables for RACF Secured Signon	300
9. Translation Table for RACF Secured Signon	300
10. Secured Signon Session Key Generation Logic	304
11. CDMF Key-Weakening Logic	305

About this document

This document supports z/OS (5694–A01) and z/OS.e (5655–G52).

This document contains information about Resource Access Control Facility (RACF), which is a component of Security Server. The Security Server is comprised of the following components:

- Resource Access Control Facility (RACF)
- DCE Security Server
- z/OS Firewall Technologies
- Lightweight Directory Access Protocol (LDAP) Server, which includes client and server function
- Open Cryptographic Enhanced Plug-ins (OCEP)
- Network Authentication Service
- PKI Services

For information about the other components, see the publications related to those components.

This publication contains a description (including syntax and related information) of macros provided with RACF. In addition, this publication provides information on coding the interfaces used to invoke RACF from the RACF ISPF panels.

It does not document the RACROUTE macro and the independent RACF system macros (such as RACHECK, RACDEF, and RACINIT) that are documented in *z/OS Security Server RACROUTE Macro Reference*. RACF callable services and their associated data areas are documented in *z/OS Security Server RACF Callable Services*.

Intended audience

This publication is intended for use by system programmers or installation personnel for:

- Installing RACF
- Maintaining RACF databases
- Writing, testing, and installing RACF exits
- Modifying the RACF program product to satisfy the installation's particular needs

Readers of this publication should be familiar with the information in *z/OS Security Server RACF Security Administrator's Guide*, *z/OS Security Server RACROUTE Macro Reference*, and *z/OS Security Server RACF System Programmer's Guide*.

z/OS Security Server RACF Auditor's Guide, which describes the RACF report writer, might also be useful.

How to use this document

The major sections of this document contain information on the RACF product macros and interface information. Each description includes:

- A general description of the service that the macro performs,
- A table of syntax rules that you must follow when you code the macro,

Preface

- A list of the parameters you can specify and an explanation of each parameter.
- **Chapter 1, “RACF Customization Macros”**, provides information on the macros that are part of the RACF product and are necessary to its operation. System programmers can use these macros to tailor RACF to meet the needs of your installation in various ways. For example, they can add additional classes to the class descriptor table via the ICHERCDE macro.
- **Chapter 2, “Panel Driver Interface”**, describes how installations can implement a panel driver interface between an application program and the RACF panels.
- **Chapter 3, “Profile Name List Service Routine”**, describes how installations using TSO/E can use IRRPNL00 to call RACF to retrieve the names of profiles.
- **Chapter 4, “Date Conversion Routine”**, describes the Date Conversion Routine, how to invoke it and the format of a Returned Converted Date.
- **Chapter 5, “SMF Records”**, contains information on SMF record types 80, 81, and 83 as well as reformatted RACF SMF records.
- **Chapter 6, “RACF SMF Data Unload Utility (IRRADU00)”**, contains detailed descriptions of the records produced by the RACF SMF data unload utility.
- **Chapter 10, “RACF Database Unload Utility (IRRDBU00)”**, contains detailed descriptions of the records produced by the RACF database unload utility.
- **Chapter 11, “The RACF Secured Signon PassTicket”**, describes the PassTicket, an alternative to the RACF password.
- **Chapter 12, “The RACF Environment Service”**, contains the Environment Service functions, descriptions, requirements and parameters.
- **Appendix A, “ICHEINTY, ICHETEST, and ICHEACTN Macros”**, provides information on the ICHEINTY macro and the macros that work as part of it: ICHETEST and ICHEACTN. Very experienced programmers who want to write their own code to interface with the RACF database can use these macros to do so. Given the level of complexity of the ICHEINTY macro, however, it is recommended that you use the RACROUTE REQUEST=EXTRACT macro instead.
- **Appendix B, “REXX RACVAR”**, describes the RACF service for REXX EXECs that provides information about the running user.
- **Appendix C, “IBM-supplied class descriptor table entries”**, lists the class entries supplied by IBM in the class descriptor table (ICHRRCDX).
- **Appendix D, “RACF database templates”**, contains database templates.
- **Appendix E, “Event Code Qualifier Descriptions”**, contains detailed explanations of the SMF event code qualifiers.
- **Appendix G, “Notices”**, contains copyright and trademark information.

Where to find more information

Where necessary, this document references information in other publications. For complete titles and order numbers for all elements of z/OS™, see *z/OS Information Roadmap*.

Softcopy publications

The RACF® library is available on the following CD-ROMs. The CD-ROM online library collections include Library Reader™, which is a program that enables you to view the softcopy documents.

SK3T-4269 *z/OS Version 1 Release 4 Collection*

This collection contains the set of unlicensed documents for the current release of z/OS in both BookManager® and Portable Document Format (PDF) files. You can view or print the PDF files with the Adobe Acrobat reader.

SK3T-4272 *z/OS Security Server RACF Collection*

This softcopy collection kit contains the Security Server library for z/OS in both BookManager and Portable Document Format (PDF) files. You can view or print the PDF files with the Adobe Acrobat reader.

SK2T-2180 *Online Library OS/390 Security Server RACF Information Package*

This softcopy collection contains the Security Server library for OS/390. It also contains the RACF/MVS Version 2 product libraries, the RACF/VM 1.10 product library, product documents from the OS/390® and VM collections, International Technical Support Organization (ITSO) documents (known as Redbooks™), and Washington System Center (WSC) documents (known as orange books) that contain information related to RACF. The collection does not contain any licensed publications. By using this CD-ROM, you have access to RACF-related information from IBM products such as OS/390, VM/ESA®, CICS®, and NetView®.

SK3T-7876 *IBM eServer zSeries™ Redbooks Collection*

This softcopy collection contains a set of documents called Redbooks that pertain to zSeries subject areas ranging from e-business application development and enablement to hardware, networking, Linux, solutions, security, Parallel Sysplex® and many others.

SK2T-2177 *IBM Redbooks S/390® Collection*

This softcopy collection contains a set of documents called Redbooks that pertain to S/390 subject areas ranging from application development and enablement to hardware, networking, security, Parallel Sysplex and many others.

RACF courses

The following RACF classroom courses are available:

- ES840** *Implementing RACF Security for CICS/ESA® and CICS/TS*
- H3917** *Basics of OS/390 Security Server RACF Administration*
- H3927** *Effective RACF Administration*
- ES88A** *Exploiting the Features of OS/390 Security Server RACF*

IBM provides a variety of educational offerings for RACF. For more information about classroom courses and other offerings, do any of the following:

- See your IBM representative
- Call 1-800-IBM-TEACH (1-800-426-8322)

Using LookAt to look up message explanations

LookAt is an online facility that allows you to look up explanations for most messages you encounter, as well as for some system abends and codes. Using LookAt to find information is faster than a conventional search because in most cases LookAt goes directly to the message explanation.

Preface

You can access LookAt from the Internet at:

<http://www.ibm.com/eserver/zseries/zos/bkserv/lookat/>

or from anywhere in z/OS where you can access a TSO/E command line (for example, TSO/E prompt, ISPF, z/OS UNIX System Services running OMVS). You can also download code from the *z/OS Collection* (SK3T-4269) and the LookAt Web site that will allow you to access LookAt from a handheld computer (Palm Pilot VIIx suggested).

To use LookAt as a TSO/E command, you must have LookAt installed on your host system. You can obtain the LookAt code for TSO/E from a disk on your *z/OS Collection* (SK3T-4269) or from the **News** section on the LookAt Web site.

Some messages have information in more than one document. For those messages, LookAt displays a list of documents in which the message appears.

Accessing z/OS licensed documents on the Internet

z/OS licensed documentation is available on the Internet in PDF format at the IBM Resource Link™ Web site at:

<http://www.ibm.com/servers/resourceLink>

Licensed documents are available only to customers with a z/OS license. Access to these documents requires an IBM Resource Link user ID and password, and a key code. With your z/OS order you received a Memo to Licensees, (GI10-0671), that includes this key code.

To obtain your IBM Resource Link user ID and password, log on to:

<http://www.ibm.com/servers/resourceLink>

To register for access to the z/OS licensed documents:

1. Sign in to Resource Link using your Resource Link user ID and password.
2. Select **User Profiles** located on the left-hand navigation bar.

Note: You cannot access the z/OS licensed documents unless you have registered for access to them and received an e-mail confirmation informing you that your request has been processed.

Printed licensed documents are not available from IBM.

You can use the PDF format on either **z/OS Licensed Product Library CD-ROM** or IBM Resource Link to print licensed documents.

IBM systems center publications

IBM systems centers produce documents known as red and orange books that can help you set up and use RACF. These documents have not been subjected to any formal review nor have they been checked for technical accuracy, but they represent current product understanding (at the time of their publication) and provide valuable information on a wide range of RACF topics. They are not shipped with RACF; you must order them separately. A selected list of these documents follows. Other documents are available, but they are not included in this list, either because the information they present has been incorporated into IBM product manuals or because their technical content is outdated.

G320-9279 *Systems Security Publications Bibliography*
GG22-9396 *Tutorial: Options for Tuning RACF*

GG24-3378	<i>DFSMS and RACF Usage Considerations</i>
GG24-3451	<i>Introduction to System and Network Security: Considerations, Options, and Techniques</i>
GG24-3524	<i>Network Security Involving the NetView Family of Products</i>
GG24-3970	<i>Elements of Security: RACF Overview - Student Notes</i>
GG24-3971	<i>Elements of Security: RACF Installation - Student Notes</i>
GG24-3972	<i>Elements of Security: RACF Advanced Topics - Student Notes</i>
GG24-3984	<i>RACF Macros and Exit Coding</i>
GG24-4282	<i>Secured Single Signon in a Client/Server Environment</i>
GG24-4453	<i>Enhanced Auditing Using the RACF SMF Data Unload Utility</i>
GG26-2005	<i>RACF Support for Open Systems Technical Presentation Guide</i>
GC28-1210	<i>System/390® MVS™ Sysplex Hardware and Software Migration</i>
SG24-4704	<i>OS/390 Security Services and RACF-DCE Interoperation</i>
SG24-4820	<i>OS/390 Security Server Audit Tool and Report Application</i>
SG24-5158	<i>Ready for e-business: OS/390 Security Server Enhancements</i>
SG24-5339	<i>The OS/390 Security Server Meets Tivoli®: Managing RACF with Tivoli Security Products</i>

Other sources of information

IBM provides customer-accessible discussion areas where RACF may be discussed by customer and IBM participants. Other information is also available through the Internet.

IBM discussion areas

IBM provides *ibm.servers.mvs.racf* newsgroup for discussion of RACF-related topics. You can find this newsgroup on news (NNTP) server *news.software.ibm.com* using your favorite news reader client.

Internet sources

The following resources are available through the Internet to provide additional information about the RACF library and other security-related topics:

- **Online library**

To view and print online versions of the z/OS publications, use this address:
<http://www.ibm.com/servers/eserver/zseries/zos/bkserv/>

- **Redbooks**

The documents known as Redbooks that are produced by the International Technical Support Organization (ITSO) are available at the following address:
<http://www.ibm.com/redbooks/>

- **Enterprise systems security**

For more information about security on the S/390 platform, OS/390, and z/OS, including the elements that comprise the Security Server, use this address:
<http://www.ibm.com/servers/eserver/zseries/zos/security/>

- **RACF home page**

You can visit the RACF home page on the World Wide Web using this address:
<http://www.ibm.com/servers/eserver/zseries/zos/racf/>

- **RACF-L discussion list**

Customers and IBM participants may also discuss RACF on the RACF-L discussion list. RACF-L is not operated or sponsored by IBM; it is run by the University of Georgia.

To subscribe to the RACF-L discussion and receive postings, send a note to:
listserv@listserv.uga.edu

Preface

Include the following line in the body of the note, substituting your first name and last name as indicated:

```
subscribe racf-l first_name last_name
```

To post a question or response to RACF-L, send a note, including an appropriate Subject: line, to:

```
racf-l@listserv.uga.edu
```

- **Sample code**

You can get sample code, internally-developed tools, and exits to help you use RACF. This code works in our environment, at the time we make it available, but is not officially supported. Each tool or sample has a README file that describes the tool or sample and any restrictions on its use.

To access this code from a Web browser, go to the RACF home page and select the “Downloads” topic from the navigation bar, or go to <ftp://ftp.software.ibm.com/eserver/zseries/zos/racf/>.

The code is also available from [ftp.software.ibm.com](ftp://ftp.software.ibm.com) through anonymous FTP. To get access:

1. Log in as user **anonymous**.
2. Change the directory, as follows, to find the subdirectories that contain the sample code or tool you want to download:

```
cd eserver/zseries/zos/racf/
```

An announcement will be posted on the RACF-L discussion list and on newsgroup *ibm.servers.mvs.racf* whenever something is added.

Note: Some Web browsers and some FTP clients (especially those using a graphical interface) might have problems using [ftp.software.ibm.com](ftp://ftp.software.ibm.com) because of inconsistencies in the way they implement the FTP protocols. If you have problems, you can try the following:

- Try to get access by using a Web browser and the links from the RACF home page.
- Use a different FTP client. If necessary, use a client that is based on command line interfaces instead of graphical interfaces.
- If your FTP client has configuration parameters for the type of remote system, configure it as UNIX[®] instead of MVS.

Restrictions

Because the sample code and tools are not officially supported,

- There are no guaranteed enhancements.
- No APARs can be accepted.

To request copies of IBM publications

Direct your request for copies of any IBM publication to your IBM representative or to the IBM branch office serving your locality.

There is also a toll-free customer support number (1-800-879-2755) available Monday through Friday from 6:30 a.m. through 5:00 p.m. Mountain Time. You can use this number to:

- Order or inquire about IBM publications
- Resolve any software manufacturing or delivery concerns

Preface

- Activate the program reorder form to provide faster and more convenient ordering of software updates

Preface

Summary of Changes

Summary of changes for SA22-7681-03 z/OS Version 1 Release 4

This book contains information previously presented in *z/OS Security Server RACF System Programmer's Guide*, SA22-7681-02, which supports z/OS Version 1 Release 3.

New information

- Information is added to indicate that this document supports z/OS (5694–A01) and z/OS.e (5655–G52)
- LDAPBIND class
- SMF data types to support PKI
- Two ACCESS qualifiers
- IRRENS00 function codes and function flags, and ICHRFROX routine code
- The general resource EIM record, which defines EIM-related information
- Data Type 6 event code 24 bit added to support EIMREGISTRY and NOEIMREGISTRY
- Data Type 6 event code 66 bit added to support the PCICC keyword

Changed information

- Invoking secured signon description of *appname*

Starting with z/OS Version 1 Release 2, you might notice changes in the style and structure of some content in this book—for example, headings that use uppercase for the first letter of initial words only, and procedures that have a different look and format. The changes are ongoing improvements to the consistency and retrievability of information in our books.

This book includes terminology, maintenance, and editorial changes. Technical changes or additions to the text are indicated by a vertical line to the left of the change.

Summary of Changes for SA22-7682-02 z/OS Version 1 Release 3

This book contains information previously presented in *z/OS Security Server RACF Macros and Interfaces*, SA22-7682-01, which supports z/OS Version 1 Release 2.

New Information

- Chapter 6, “RACF SMF Data Unload Utility (IRRADU00)” on page 113 was updated to add the:
 - PDACCESS event qualifiers and record extensions in support of Policy Director Authorization Services Support.
 - SETFACL and DELFACL event qualifiers and record extensions in support of Access Control Lists.
 - RPKIREAD, RPKIUPDR, and RPKIUPDC event qualifiers and record extensions in support of PKI Services.

- Chapter 5, “SMF Records” on page 35 was updated to reflect changes in support of Access Control Lists, PKI Services, and Policy Director Authentication Services.
 - The following event codes were added:
 - 69(45)** R_PKIServ GENCERT
 - 70(46)** R_PKIServ EXPORT
 - 71(47)** Policy Director Control Decision
 - 72(48)** R_PKIServ QUERY, DETAILS, VERIFY
 - 73(49)** R_PKIServ UPDATEREQ
 - 74(4A)** R_PKIServ UPDATECERT, REVOKE
 - 75(4B)** SETFACL
 - 76(4C)** DELFACL
- An appendix with z/OS product accessibility information has been added.

Changed Information

- “The RACF Router Table Supplied by IBM (ICHRFR0X)” on page 21 was updated to add an entry for the CACHECLS class.
- Support of FMID 7706 for z/OS Version 1 Release 3 was added to the following fields:
 - SMF80VRM
 - SMF81VRM
 - SMF83VRM
- Chapter 10, “RACF Database Unload Utility (IRRDBU00)” on page 249 was updated to reflect the following changes:
 - User PROXY record (02E0)
 - General resource PROXY record (0590)
- Appendix A, “ICHEINTY, ICHETEST, and ICHEACTN Macros” on page 313 was updated to reflect support of FMID 7706 for z/OS Version 1 Release 3 on the RELEASE operand of the following macros:
 - ICHEINTY
 - ICHETEST
 - ICHEACTN
- Appendix C, “IBM-supplied class descriptor table entries” on page 351 was updated to add entries for the following classes:
 - CACHECLS
 - PRINTSRV

This book includes terminology, maintenance, and editorial changes. Technical changes or additions to the text are indicated by a vertical line to the left of the change.

Starting with z/OS Version 1 Release 2, you might notice changes in the style and structure of some content in this book—for example, headings that use uppercase for the first letter of initial words only, and procedures that have a different look and format. The changes are ongoing improvements to the consistency and retrievability of information in our books.

Summary of Changes for SA22-7682-01 z/OS Version 1 Release 2

This book contains information previously presented in *z/OS Security Server RACF Macros and Interfaces*, SA22-7682-00, which supports z/OS Version 1 Release 1.

New Information

- “ICHNCONV Coding Recommendation” on page 9

Changed Information

- “ICHERCDE Macro” on page 1 was updated to include the CASE operand in support of mixed-case profile names.
- “The RACF Router Table Supplied by IBM (ICHRFR0X)” on page 21 was updated to add entries for the following classes:
 - EJBROLE
 - GDSNJR
 - GEJBROLE
 - MDSNJR
- Chapter 5, “SMF Records” on page 35 was updated to reflect the following changes:
 - Relocate section 13 was added to the following event codes:
 - 8(8) ADDSD**
 - 21(15) RDEFINE**
 - Support of FMID 7705 for z/OS Version 1 Release 2 was added to the following fields:
 - SMF80VRM
 - SMF81VRM
 - SMF83VRM
 - A flag was added to the data type 6 record for event code 9(9) in support of the UNIVERSAL operand of the ADDGROUP command.
 - Field SMF81KBL was added to record type 81 in support of SETROPTS KERBLVL processing for Network Authentication Service.
- Chapter 6, “RACF SMF Data Unload Utility (IRRADU00)” on page 113 was updated to add the RINI_KERBLVL field in support of SETROPTS KERBLVL processing for Network Authentication Service.
- Chapter 10, “RACF Database Unload Utility (IRRDBU00)” on page 249 was updated to reflect the following changes:
 - GPBD_UNIVERSAL field was added to the Group Basic data record (0100) in support of universal groups.
 - The following fields were added to the User KERB (02D0) and General Resource KERB (0580) data records in support of SETROPTS KERBLVL processing for Network Authentication Service:
 - USKERB_ENCRYPT_DES
 - USKERB_ENCRYPT_DES3
 - USKERB_ENCRYPT_DESD
 - The description of the GRBD_UACC field of the General Resource Basic data record (0500) was updated to include the following UACC values for profiles in the DIGTCERT class:
 - TRUST
 - NOTRUST
 - HIGHTRST
- Appendix A, “ICHEINTY, ICHETEST, and ICHEACTN Macros” on page 313 was updated to reflect support of FMID 7705 for z/OS Version 1 Release 2 z/OS on the RELEASE operand of the following macros:
 - ICHEINTY
 - ICHETEST
 - ICHEACTN

- Appendix C, “IBM-supplied class descriptor table entries” on page 351 was updated to add entries for the following classes:
 - EJBROLE
 - GDSNJR
 - GEJBROLE
 - MDSNJR
- Appendix D, “RACF database templates” on page 391 was updated to reflect the following changes:
 - The UNVFLG field was added to the BASE segment of the GROUP template in support of universal groups.
 - The ENCRYPT field was added to the KERB segment of the following templates in support of SETROPTS KERBLVL processing for Network Authentication Service:
 - USER
 - GENERAL

Reorganized Information

- Chapter 12, “The RACF Environment Service” on page 307

Starting with z/OS Version 1 Release 2, you might notice changes in the style and structure of some content in this book—for example, headings that use uppercase for the first letter of initial words only, and procedures that have a different look and format. The changes are ongoing improvements to the consistency and retrievability of information in our books.

This book includes terminology, maintenance, and editorial changes. Technical changes or additions to the text are indicated by a vertical line to the left of the change.

Chapter 1. RACF Customization Macros

This chapter contains information that is *not* a programming interface. It is intended to help the installations that use RACF product macros to customize a RACF installation.

This chapter describes the following macros that are available for use by your installation.

- “**ICHERCDE Macro**”—used to generate entries for the resource class descriptor table.
- “**ICHNCONV Macro**” on page 9—used to create the installation’s naming convention table.
- “**ICHRFRTB Macro**” on page 20—used to generate entries in the RACF router table.

For the descriptions and functions of the ICHEINTY, ICHETEST, and ICHEACTN product macros that are used to locate, update, test, and retrieve various profiles in the RACF database see Appendix A, “ICHEINTY, ICHETEST, and ICHEACTN Macros” on page 313.

Recommendation: Because of the complexity of these macros and the cautions required in their use, you should use the RACROUTE REQUEST=EXTRACT system macro instead. See *z/OS Security Server RACROUTE Macro Reference* for more information.

ICHERCDE Macro

The ICHERCDE macro generates entries for the resource class descriptor table. The class descriptor table contains information that directs the processing of general resources. The table consists of an entry for each class except USER, GROUP, and DATASET. To generate the table, you must invoke the macro once for each class. To identify the end of the class descriptor table, you invoke the macro without specifying any operands.

The class descriptor table has two parts. IBM supplies ICHRRCDX, which must not be modified. The installation optionally supplies ICHRRCDE, which must have RMODE(24). ICHRRCDE must reside in SYS1.LINKLIB or another library in your linklist concatenation. Refer to *z/OS Security Server RACF System Programmer’s Guide* for instructions on how to create ICHRRCDE.

Member RACINSTL in SYS1.SAMPLIB, contains among other items, a sample job stream for updating or creating an installation-defined class descriptor table (ICHRRCDE).

Notes:

1. Any installation planning to use RACROUTE to process classes which the installation has added, must either
 - Code an ICHRFRTB macro instruction for each entry added to the class descriptor table to be accessed by the RACROUTE macro instruction, or
 - Specify DECOUPL=YES on the RACROUTE macro instruction itself

in order for RACROUTE to process the added classes. See “ICHRFRTB Macro” on page 20.

ICHERCDE macro

2. Before adding a user-defined entry to the class descriptor table, a corresponding entry must be present in the RACF router table. The RACF router table entries are made as follows:
 - a. If the class has RACLIST=ALLOWED, use ICHRFRTB to create a router table entry. Code the ICHRFRTB macro with ACTION=RACF and specify blanks for both the REQSTOR= and the SUBSYS= parameters so that RACF can process the class if you issue a SETROPTS RACLIST command.
 - b. If your application uses RACROUTE, and requires REQSTOR= and SUBSYS=, you will need to code an additional ICHRFRTB macro specifying ACTION=RACF and the appropriate requester and subsystem values.
3. A maximum of 1024 classes can be defined in the class descriptor table; 438 of these are available for installation use, and 586 are reserved for use by IBM. There are 1024 POSIT values, of which numbers 19–56 and 128–527 are available for installation use. Numbers 0–18, 57–127, and 528–1023 are reserved for IBM use.
4. Installations sharing a database do not need identical class-descriptor tables, but they must be compatible. If the same class is present on multiple systems, it must have the same attributes; for example, the POSIT numbers must be the same. Therefore, if systems X and Y are sharing a database, and system X has a class-descriptor table with classes a, b, and c, and system Y has a class-descriptor table with classes a, b, c, d, e, and f, the classes a, b, and c must be defined identically on both systems. However, system Y may have classes d, e, and f that are not defined on system X. Note that when RACF is enabled for sysplex communication, to allow flexibility when adding new classes to the class-descriptor table RACF does not enforce consistency in the class-descriptor table as it does with the data set name table and the range table.

Once a class-descriptor table is assembled on RACF 2.2, that ICHRRCDE module cannot be used on lower-level systems. For more information, see *z/OS Security Server RACF System Programmer's Guide*.

The ICHERCDE macro produces a CSECT for each invocation. If the CLASS operand is present, the CSECT name is the name of the class being defined; otherwise, the CSECT name is ICHRRCDE.

The ICHERCDE macro definition is as follows:

```
[label] ICHERCDE [CLASS=classname]
                [,CASE=UPPER|ASIS]
                [,DFTRETC=0|4|8]
                [,DFTUACC=ALTER|CONTROL|UPDATE|READ|NONE]
                [,FIRST=ALPHA|NUMERIC|ALPHANUM|ANY|
                NONATABC|NONATNUM]
                [,GENLIST=ALLOWED|DISALLOWED]
                [,GROUP=group-class|MEMBER=member-class]
                [,ID=number]
                [,KEYQUAL=0|nnn]
                [,MAXLENX=number]
                [,MAXLNTH=8|number]
                [,OPER=YES|NO]
                [,OTHER=ALPHA|NUMERIC|ALPHANUM|ANY|
                NONATABC|NONATNUM]
                [,POSIT=number]
                [,PROFDEF=YES|NO]
                [,RACLIST=ALLOWED|DISALLOWED]
                [,RACLREQ=YES|NO]
                [,RVRSMAC=YES|NO]
                [,SLBLREQ=YES|NO]
```

CLASS=class name

Specifies the name of the resource class. The name must be 4–8 characters long and must consist of the following: A through Z, 0 through 9, or # (X'7B'), @ (X'7C'), \$ (X'5B'). The first character must be A through Z, # (X'7B'), @ (X'7C'), or \$ (X'5B'). You must include a # (X'7B'), @ (X'7C'), \$ (X'5B'), or numeric character in the name of any class you define in order to guarantee that installation-defined classes do not conflict with classes supplied by IBM. In this way, classes supplied by IBM should always have unique class names. If this rule is not followed, the assembler issues a severity 4 MNOTE warning.

If you specify any options on the ICHERCDE macro, you must specify the CLASS operand.

CASE=UPPER | ASIS

Specifies whether mixed-case profile names are allowed for the class specified by the CLASS operand. UPPER is the default. When ASIS is specified, RACF commands preserve the case of profile names for the specified class. Lowercase characters are allowed in any position of the profile name where alphabetic characters are allowed, based on the character restrictions specified in the FIRST= and OTHER= operands.

DFTRETC=0|4|8

Specifies the return code that RACF will provide from RACROUTE REQUEST=AUTH, or REQUEST=FASTAUTH when RACF and the class are active and (if required) the class has been processed using SETROPTS RACLIST, but RACF doesn't find a profile to protect the resource specified on the AUTH or FASTAUTH request.

- 0** The access request was accepted.
- 4** No profile exists.
- 8** The access request was denied.

If you do not specify this parameter, it defaults to 4.

DFTUACC= ALTERICONTROLIUPDATEIREADINONE

Specifies the minimum access allowed if the access level is not set when a resource profile is defined in the class. If you omit DFTUACC, and no access level is specified at the time the profile is created, RACF uses the default universal access authority from the command issuer's ACEE.

FIRST=

Specifies a character type restriction for the first character of the profile name.

- ALPHA** Specifies an alphabetic, # (X'7B'), @ (X'7C'), or \$ (X'5B'). ALPHA is the default value for both the FIRST and OTHER operand.
- NUMERIC** Specifies a digit (0–9).
- ALPHANUM** Specifies an alphabetic, a numeric, # (X'7B'), @ (X'7C'), or \$ (X'5B').
- ANY** Specifies any character other than a blank, a comma, a parenthesis, or a semicolon.

Note: Resource names (as opposed to profile names) for a class should not contain the characters *, %, or & since these characters do not work as expected when generic profile processing is active for the class.

- NONATABC** Specifies an alphabetic character. Characters such as # (X'7B'), @ (X'7C'), \$ (X'5B'), and numerics are excluded.

ICHERCDE macro

NONATNUM Specifies an alphabetic or numeric character. Characters such as # (X'7B'), @ (X'7C'), and \$ (X'5B') are excluded.

GENLIST=ALLOWED|DISALLOWED

Specifies whether `SETROPTS GENLIST` is to be allowed for the class. If you `GENLIST` the class on the `SETROPTS` command, then if a user requests access to a resource protected by a generic profile, a copy of that profile will be brought into the common storage area, rather than into the user's address space. RACF uses those generic profiles in common storage to check the authorization of any users who want to access the resource. The profiles remain in common storage until a `REFRESH` occurs.

GROUP=group-class

Specifies the name of the class that groups the resources within the class specified by the `CLASS` operand. If you omit this operand, RACF does not allow resource grouping for the resource specified by the `CLASS` operand. If group is specified, the group entry must be in the same class descriptor table (CDT) as the member entry (IBM or installation).

ID=number

Specifies a number from 1 to 255 that is associated with the class name. RACF stores this number in the general profile. Numbers 1 through 127 are reserved for use by IBM; numbers 128 through 255 are reserved for use by the installation.

The ID keyword need not be unique for each class; in fact, if more than 128 class descriptor table entries are defined by the installation, ID numbers will have to be reused. An installation can use ID numbers to identify related classes; however, RACF does not use the ID number. Do not confuse the ID number with the `POSIT` number described below.

If you specify any options on the `ICHERCDE` macro, you must specify the ID operand.

KEYQUAL=nnn

Specifies the number of matching qualifiers RACF uses when loading generic profile names to satisfy an authorization request if a discrete profile does not exist for the resource. For example, if you specify two for the class, all generic profile names whose two highest level qualifiers match the two highest qualifiers of the entity name are loaded into the user's storage when the user requests access to a resource.

If you do not specify `KEYQUAL`, the default is 0, and profile names for the entire class are loaded and searched. The maximum value you can specify for `KEYQUAL` is 123, which is the maximum number of qualifiers in a name 246 characters long.

When `KEYQUAL=nnn` is coded in the `ICHERCDE` macro, generic profiles created in that class may not contain generic characters in the first *nnn* qualifiers of the profile.

MAXLENX=number

Specifies the maximum length of resource and profile names for this class when a `RACROUTE` macro is invoked with the `ENTITYX` keyword, or a profile is added or changed via a RACF command processor. For installation-defined classes you can specify a number from 1 to 246. If `MAXLENX` is not specified, the value specified for `MAXLNTH` is used.

Notes:

1. Do not assemble a class descriptor table using `MAXLENX` and share it with a system running a RACF release earlier than OS/390 V2R8.

2. If you specify a MAXLENX value greater than the MAXLNTH value for a class, before you define any profiles with names longer than MAXLNTH, you should verify that any programs using RACROUTE REQUEST=EXTRACT, TYPE=EXTRACTN or ICHEINTY NEXT for that class will properly handle the longer names.

MAXLNTH=8|number

Specifies the maximum length of resource and profile names for this class when MAXLENX is not specified. When MAXLENX is also specified, MAXLNTH represents the maximum length of a resource name only when a RACROUTE macro is invoked with the ENTITY keyword. For installation-defined classes, you can specify a number from 1 to 246; the default is 8.

Note: You cannot use the MAXLNTH or MAXLENX parameters to change the maximum size allowed for a resource name by the resource manager. For example, CICS allows a maximum of 13 characters in a transaction name. Thus, if you define additional CICS transaction classes, you must also specify MAXLNTH=13.

This restriction does **not** apply to transaction grouping classes.

MEMBER=member-class

Specifies the name of the class grouped by the resources within the class specified by the CLASS operand. The class name must be from 1 to 8 alphanumeric characters. When this operand is specified, the class being defined is a resource group. If a member is specified, the member entry must be in the same class descriptor table (CDT), (IBM or installation) as the group entry.

OPER=YES|NO

Specifies whether RACF is to take the OPERATIONS attribute into account when it performs authorization checking. If YES is specified, RACF considers the OPERATIONS attribute; if NO is specified, RACF ignores the OPERATIONS attribute. YES is the default.

OTHER=

Specifies a character type restriction for the characters of the profile name other than the first character.

ALPHA Specifies an alphabetic or # (X'7B'), @ (X'7C'), \$ (X'5B'). ALPHA is the default value for both the FIRST and OTHER operand.

NUMERIC Specifies a digit (0–9).

ALPHANUM Specifies an alphabetic, numeric, or # (X'7B'), @ (X'7C'), \$ (X'5B').

ANY Specifies any character other than a blank, comma, a parenthesis, or semicolon.

Note: Resource names (as opposed to profile names) for a class should not contain the characters *, %, or & since these characters do not work as expected when generic profile processing is active for the class.

NONATABC Specifies an alphabetic character. Characters such as # (X'7B'), @ (X'7C'), \$ (X'5B'), and numerics are excluded.

NONATNUM Specifies an alphabetic or numeric character. Characters such as # (X'7B'), @ (X'7C'), and \$ (X'5B') are excluded.

ICHERCDE macro

POSIT=number

Specifies the POSIT number associated with the class. Each class in the class descriptor table has a POSIT number specified on the ICHERCDE macro. The POSIT number identifies a set of option flags that controls the following RACF processing options:

- Whether authorization checking should take place for the class (SETROPTS CLASSACT)
- Whether auditing should take place for resources within the class (SETROPTS AUDIT)
- Whether statistics should be kept for resources within the class (SETROPTS STATISTICS)
- Whether generic profile access checking is active for the class (SETROPTS GENERIC)
- Whether generic command processing is active for the class (SETROPTS GENCMD)
- Whether global access checking is active for the class (SETROPTS GLOBAL)
- Whether user has CLAUTH to a resource class
- Whether special resource access auditing applies to the class (SETROPTS LOGOPTIONS)
- Whether SETROPTS RACLIST will occur for this class (when the parameter RACLIST=ALLOWED is also coded)

Before you assemble the class descriptor table (CDT), you must decide whether to use a unique set of option flags for each RACF class or whether to have two or more RACF classes share the same set of option flags.

If you choose to use a unique set of option flags for a class, assign the class a unique POSIT number. If you choose to share the same set of option flags among several classes, assign those classes the same POSIT number. After creating your class descriptor table, you can activate the classes that comprise it and their respective set of option flags via the appropriate keywords on the SETROPTS command.

Recommendation: A RACF class that has a default return code of 8 should not share a POSIT value with a RACF class having a default return code not equal to 8. If a class with a default return code of 8 is activated but no profiles are defined, user activity that requires access in that class will be prevented.

There are 1024 POSIT numbers that can identify 1024 sets of option flags. Installations can specify POSIT numbers 19–56 and 128–527. Numbers 0–18, 57–127, and 528–1023 are reserved for IBM use.

Adding a New Class Where a Unique POSIT Number Is Desired: Suppose you decide to define a new class called \$TSTCLAS. Since you want this class to be administered separately from any other class, you select a new POSIT number, 22, which is not being used by any other class in ICHRRCDE. Now, when you activate or deactivate SETROPTS options for \$TSTCLAS, or grant CLAUTH to this class, no other classes are affected.

Adding a New Class That Shares a POSIT Number with an Existing Class: Suppose you have a class called \$PONIES that was previously defined with a unique POSIT number, 21. SETROPTS CLASSACT, SETROPTS AUDIT, and

SETROPTS STATISTICS are currently in effect on your system for class \$PONIES as a result of issuing those commands for class \$PONIES.

Later, you decide to define the class of \$HORSES, a class related to \$PONIES, and logically requiring the same RACF processing options. Therefore, when you code the ICHERCDE macro to include the \$HORSES class in the class descriptor table, specify the POSIT number as 21, the same as for \$PONIES.

Now when you IPL with new ICHRRCDE, the same RACF processing options that are in effect for class \$PONIES will automatically be in effect for the new class \$HORSES: SETROPTS CLASSACT, SETROPTS AUDIT, and SETROPTS STATISTICS.

Further, issuing either

- SETROPTS GLOBAL(\$PONIES) or
- SETROPTS GLOBAL(\$HORSES)

activates global access checking for both the \$PONIES and the \$HORSES classes. Similarly, either

- SETROPTS STATISTICS(\$PONIES) or
- SETROPTS STATISTICS(\$HORSES)

activates STATISTICS for both the \$PONIES and the \$HORSES classes.

Any number of classes may share the same POSIT number. For example, a third class called \$MARES could be added and could also share POSIT number 21 with \$PONIES and \$HORSES. Sharing a POSIT number simplifies administration of related classes.

Because you have specified the same POSIT number for both \$PONIES and \$HORSES (the classes share the same option flag), you do not need to reissue the command to activate the same set of options for \$HORSES. RACF does it automatically because a relationship has been established between the POSIT number (on the ICHERCDE macro) and the set of options it represents (activated on the SETROPTS command.)

Be aware that if two or more classes share the same POSIT number, and you make a change to the option flag set of one of the classes via the SETROPTS command, the change will also be in effect for all the classes that share that POSIT number. Thus, if you turn off statistics options for the class of \$PONIES, that action turns off statistics for the class of \$HORSES because both classes share the same POSIT number. You must code a unique POSIT number for each class if you want RACF to independently control processing options.

Changing an Existing Installation-Defined Class: If you change the POSIT value, follow up with the SETROPTS LIST command, since changing the POSIT value could cause unpredictable results. For example, you could deactivate a class if you change it to use a POSIT value associated with a class that is not active.

If you are changing the POSIT value, do the following before making the change:

1. Use SETR LIST and record each active option for the class.

ICHERCDE macro

2. Examine your classes to see if any other class is using the current POSIT value. If not, use SETR to turn off all the options associated with the class, so that you won't get any extraneous options set if you later add a class using that POSIT value.
3. After you make the change, and have re-IPLed all the systems that will be using the new class, use SETROPTS to set any of the options that are still relevant for the class, using the output of the previous SETR LIST as reference.

Deleting an Installation-Defined Class: You can delete a class entry from the descriptor table by specifying the name of the class to be deleted on the OS-linkage-editor REPLACE statement. For the deletion to take effect, re-IPL MVS.

You should ensure that all profiles relating to this class are deleted *before* deleting the class-descriptor-table entry.

Pay special attention to any *unique* POSIT values you use. If the class you are deleting has a *unique* POSIT value, issue a SETROPTS LIST to check what options you are using with the class—for example, CLASSACT, LOGOPTIONS, AUDIT, RACLIST, and so forth. Turn off each of the options for the class.

An example: You may have activated your class. You should deactivate the class before re-IPLing your system. If you do not deactivate the class and, at a future date, you create a class with the POSIT value previously used, the class will automatically be active. The same consideration applies to each option controlled by the POSIT value.

PROFDEF=YESINO

Specifies whether you want RACF to allow profiles to be defined for this RACF resource class. If you specify PROFDEF=NO, RACF will not allow profiles to be defined to this RACF resource class; if a user attempts to define a profile to that class, the RDEFINE command responds with an appropriate message.

RACLIST=ALLOWEDIDISALLOWED

Specifies whether SETROPTS RACLIST is to be allowed for the class. If you process the class using SETROPTS RACLIST, RACF brings copies of all discrete and generic profiles within that class into storage in a data space. RACF uses those profiles in storage to check the authorization of any users who want to access the resources. The profiles remain in storage until removed by SETROPTS NORACLIST.

RACLREQ=YESINO

Specifies whether you must have processed the class using SETROPTS RACLIST, either via the RACLIST macro or via SETROPTS RACLIST, in order to use RACROUTE REQUEST=AUTH. The purpose of this keyword is to allow routines that cannot tolerate I/O, to invoke RACF. If you specify YES, and the class is not processed by SETROPTS RACLIST and a RACROUTE REQUEST=AUTH is attempted, the return code is 4. If you do not specify the parameter, it defaults to NO.

RVRSMAC=YESINO

Specifies whether reverse mandatory access checking is required.

If RVRSMAC=YES is specified, RACF performs a reverse mandatory access check (MAC) when and if a mandatory access check is required. In a reverse mandatory access check, the SECLABEL of the resource must dominate that of the user.

Note that if this parameter is omitted, it is assigned the default value of RVRSMAC=NO, which means that when and if a mandatory access check is required, the user's SECLABEL must dominate that of the resource.

SLBLREQ=YES|NO

Specifies whether SECLABEL is required for the profiles of this class.

When MACTIVE is on, each profile in the class must have a SECLABEL. The default, SLBLREQ=NO, means that RACF will not require a SECLABEL for profiles in this class; however, if a SECLABEL exists for this profile, and the SECLABEL class is active, RACF will use it during authorization checking.

SLBLREQ=NO applies to general resource classes that have no profiles, such as DIRAUTH, or for classes that contain no data, such as OPERCMDS and SECLABEL.

ICHNCONV Macro

RACF requires a data set name format where the high-level qualifier of a data set name is a RACF-defined user ID or group name. If your installation's data set naming convention already meets this requirement, you should not have to use this macro.

RACF allows installations to create a naming convention table (ICHNCV00) that RACF uses to check the data set name in all the commands and SVC routines that process data set names. This table helps an installation set up and enforce data set naming conventions that are different from the standard RACF naming conventions.

RACF compares a data set name against each entry in the table until it finds one that matches the name. If RACF does not find a matching entry, the name remains unchanged.

You create a naming convention table, ICHNCV00, by using the ICHNCONV macro. You must assemble the table and link-edit it into SYS1.LPALIB. ICHNCV00 is link-edited with AMODE(31) and RMODE(ANY).

The table can have up to 400 naming convention entries and can handle data set names of different formats. Each table entry consists of:

- One ICHNCONV DEFINE macro—to start the naming convention and assign it a name
- Zero or more ICHNCONV SELECT macros—to specify the conditions when the naming convention processes the data set name
- Zero or more ICHNCONV ACTION macros—to convert the name to the standard RACF format or to change any of the modifiable variables
- One ICHNCONV END macro—to terminate the naming convention

At the end of all the naming conventions, an ICHNCONV FINAL macro terminates the table itself.

ICHNCONV Coding Recommendation

When writing a naming conventions table, be sure that your output data set names do not match any input data set names. If they match, you may receive unpredictable results. For example, suppose you have erroneous entries in your naming conventions table that transform the following input data set names to the following output data set names:

ICHNCONV macro

Poor example:

```
A.B.#ANY.THING to B#.ANY.THING
B#.ANY.THING    to C#.ANY.THING
```

When a data set named A.B.#ANY.THING is processed, it is transformed to B#.ANY.THING. If B#.ANY.THING is processed again as an input data set name, it will be transformed again, this time to C#.ANY.THING. You should avoid this type of coding in your naming convention table.

This is important because you cannot predict the input data set names that are passed to the naming convention table. In some cases, the table might receive the input data set name in "external" format, as provided by a user, such as from a LISTDSD DA(*hlq.name*) command. In other cases, it might receive the input data set name in "internal" format, as previously processed by the naming convention table, such as from an authorization check made during processing of SEARCH or LISTDSD PREFIX(*hlq*) when RACF has retrieved the data set name from the database.

ICHNCONV DEFINE

An ICHNCONV DEFINE macro starts a naming convention and assigns it a name.

The format of the ICHNCONV DEFINE macro is:

```
[label] ICHNCONV DEFINE,NAME=convention name
```

DEFINE

Identifies the start of a naming convention. The ICHNCONV DEFINE must start each naming convention and there must be only one per convention.

NAME=convention name

Specifies a unique name that you can use for the convention.

The convention name must be 1 to 8 characters long and follow the rules for symbols in assembler language.

ICHNCONV SELECT

An ICHNCONV SELECT macro specifies the conditions when the naming convention processes the data set name.

The format of the ICHNCONV SELECT macro is:

```
[label] ICHNCONV SELECT,COND=(condition|compound condition)
```

SELECT

Identifies that this convention has selection criteria.

If the condition on the COND parameter is true, the actions on the ICHNCONV ACTION macros will be processed, and processing will continue as specified on the ICHNCONV END macro. If the condition on the COND parameter is not true, RACF bypasses the ICHNCONV ACTION macros and continues with the next convention in the table.

If an ICHNCONV SELECT macro is not coded, RACF unconditionally processes the actions specified on the ICHNCONV ACTION macros, and continues as specified on the ICHNCONV END macro.

All ICHNCONV SELECT macros for a naming convention must follow the ICHNCONV DEFINE macro and precede any ICHNCONV ACTION macros.

COND=(condition)

Specifies the conditions that have to exist before the naming convention processes the data set name.

The “condition” may be a simple comparison condition of the form:

COND=(variable,operator,operand)

You can also use a “compound condition” formed by linking two or more ICHNCONV SELECT macros with logical AND and OR operators:

COND=(variable,operator,operand,AND)

or

COND=(variable,operator,operand,OR)

If a naming convention contains more than one ICHNCONV SELECT macro, all of the SELECT macros except the last must contain either AND or OR to link it to the following macro. The last (or only) ICHNCONV SELECT cannot have AND or OR specified. RACF evaluates compound conditions in the order specified. AND and OR have equal precedence. Each operation is performed in order, with no “short-circuit” evaluation. The final result of a compound condition will always be:

(...((((conv1 op1 conv2) op2 conv3) op3 conv4) op4 conv5)...opn convn+1) ...

where any “op” can be either AND or OR.

variable

Specifies the variables that the convention can reference. Valid variables are:

GQ	Input qualifiers
G	Input qualifier array subscript
UQ	Output qualifiers
U	Output qualifier array subscript
QUAL	Character qualifier
QCT	Initial number of qualifiers
NAMETYPE	Type of data set
EVENT	Event code
VOLUME	Volume serial numbers
V	Volume serial number array subscript
VCT	Number of volumes
OLDVOL	Volume serial of old volume
WKX	Temporary work variable
WKY	Temporary work variable
WKZ	Temporary work variable
WKA	Temporary work variable
WKB	Temporary work variable
WKC	Temporary work variable
RACUID	Caller’s user ID
RACGPID	Caller’s current connect group
RACUID3	User ID for third-party RACHECK
RACGPID3	Group used for the third-party RACHECK

ICHNCONV macro

RACF initializes the variables before the first convention. ICHNCONV passes any changes to a variable to subsequent conventions, but only changes made to the variables UQ, QUAL, and NAMETYPE are passed back to the RACF module that called the naming convention table processing module.

You can reference character and hexadecimal variables by substring; for example, (variable,subscript,substring-start,substring-end). If the variable does not accept subscripts or you omit the subscript, you must code a comma to show that the subscript is omitted. Variables cannot be used to define the extents of substrings. For example, (GQ,2,1,3) refers to the first three characters of the second input qualifier; (EVENT,,2,2) refers to the second byte of the event code.

Example: The definition of the data set BOB.SAMPLE.DATASET on volume 111111, when the naming convention table processing module was called during a TSO session when user RACUSR1 was connected to group RACGRP1, would lead to the following set of initial variables:

```
(GQ,1) = BOB
(GQ,2) = SAMPLE
(GQ,3) = DATASET
(GQ,4) to (GQ,22) = blank
(UQ,0) = blank
(UQ,1) = BOB
(UQ,2) = SAMPLE
(UQ,3) = DATASET
(UQ,4) to (UQ,22) = blank
QCT = 3
QUAL = BOB
NAMETYPE = UNKNOWN
EVENT = X'0201'
(VOLUME,1) = 111111
VCT = 1
G, U, V = -1
WKX, WKY, WKZ = 0
WKA, WKB, WKC = blank
OLDVOL = blank
RACUID = RACUSR1
RACUID3 = blank
RACGPID = RACGRP1
RACGPID3 = blank
```

GQ input qualifiers of the data set name.

G input qualifier array subscript.

UQ output qualifiers of the data set name.

U output qualifier array subscript.

GQ and UQ are arrays containing the qualifiers of the data set name with the high-level qualifier of the name in (GQ,1) and (UQ,1). G and U are halfword variables used to hold subscripts to the GQ and UQ arrays. G and U are initialized to negative one (-1), which is out of the range of valid subscripts.

Initially the input and output qualifiers are identical; but if the contents of the output qualifiers are changed, the new contents are used as the new data set name. Each qualifier is a 44-byte

character field padded on the right with blanks. (The field does not include the periods that separate qualifiers.) Initially, (UQ,0) is blank and is reserved for the convention to set as the new high-level qualifier.

If the name produced by the naming conventions table is longer than 44 characters, it is truncated to 44 characters. Thus, the highest possible number of qualifiers (or the highest possible value for the subscripts G and U) is 22.

Naming conventions should ensure that none of the UQ fields contain anything after the 8th position, because RACF follows the MVS JCL rules for data set names not enclosed within quotes, and requires that qualifiers be at most 8 characters in length.

If you use GQ or UQ in an ICHNCONV SELECT macro without a subscript, RACF tests the condition for each qualifier in turn until the condition is true. The variables G and U are set to the subscript of the qualifier for which the condition was true, G for the conditions using GQ and U for those involving UQ. If the condition is not true, the subscript variable will be negative one (-1).

For all conditions except NE (not equal), the implied linkage is OR; for the NE condition, the implied linkage is AND. For example,

```
SELECT COND=(GQ,EQ,'ABC')      means
```

```
SELECT COND=((GQ,0),EQ,'ABC',OR)
SELECT COND=((GQ,1),EQ,'ABC',OR) ...
```

while

```
SELECT COND=(GQ,NE,'ABC')      means
```

```
SELECT COND=((GQ,0),NE,'ABC',AND)
SELECT COND=((GQ,1),NE,'ABC',AND) ...
```

You may use any numeric variable as a subscript for GQ or UQ. If RACF encounters an out-of-range subscript (for example, -1 or 23), RACF uses blanks for the comparison.

If GQ or UQ is in an ICHNCONV ACTION macro without a subscript, RACF uses the current value of G or U respectively as the subscript.

QUAL

An 8-byte character qualifier that RACF uses in authority checking to determine if the data set is the user's data set or a group data set.

QUAL is initially the data set high-level qualifier. If the high-level qualifier is not a user ID or group name, you should set QUAL to a user ID or group name. Setting QUAL, however, is not the same as setting the data set high-level qualifier. QUAL and the high-level qualifier are two separate fields, used for different RACF processing. Therefore, if you change QUAL, you

ICHNCONV macro

probably want to set (UQ,0) to the same value as QUAL, especially for generic profile names.

QCT A 2-byte binary field containing the initial number of qualifiers in the data set name.

NAMETYPE Indicates whether the data set is a user or group data set. NAMETYPE initially has the value UNKNOWN but a convention action may set the value to be USER or GROUP. The three special constant values UNKNOWN, USER, and GROUP may be used to test and set the value of this field. NAMETYPE is available only when the caller is RACDEF.

If the convention sets the value to USER or GROUP, RACF ensures that an appropriate user or group exists and fails the RACF or ADDSD if not.

EVENT A 2-byte hexadecimal field containing the event code that is currently passed to the exit routine.

Values that EVENT may have are:

X'0100' - RACHECK (see note 1)
X'0201' - RACDEF DEFINE (RENAME new name)
X'0202' - RACDEF RENAME (OLD name)
X'0203' - RACDEF ADDVOL
X'0204' - RACDEF DELETE
X'0205' - RACDEF CHGVOL
X'0301' - ADDSD SET
X'0302' - ADDSD NOSET
X'0303' - ADDSD MODEL
X'0401' - ALTDSD SET
X'0402' - ALTDSD NOSET
X'0501' - DELDSD SET
X'0502' - DELDSD NOSET
X'0601' - LISTDSD prelocate (see note 2)
X'0602' - LISTDSD DATASET postlocate (see note 2)
X'0603' - LISTDSD ID or PREFIX postlocate (see note 2)
X'0701' - PERMIT TO-resource
X'0702' - PERMIT FROM-resource
X'0801' - SEARCH prelocate (see note 2)
X'0802' - SEARCH postlocate (see note 2)
X'0900' - IRRUT100 postlocate (see note 2)
X'0D00' - RACXTRT

Notes:

1. RACHECK may be called by the RACROUTE interface or internally by RACF commands such as LISTDSD and SEARCH. If RACHECK is invoked by the RACROUTE macro, the name passed to naming conventions is in external user-specified format. However, if the command processors call RACHECK, the name may be in either format. Since no indicator of the type of call being made is passed to the naming conventions table, the naming conventions table must determine if the name is in internal format and switch it to external format (or if the name is in external format it must switch it to internal format) for this event code.

2. Prelocate means before a profile is located; these events (as well as all of those without a note) are passed a name in the external, user-specified format.
 Postlocate means after a profile is located but before it is displayed; these events are passed a name in the internal RACF format and the naming conventions processing should include converting it back to the external, user format.
3. Error messages displayed by the command processors may use the RACF internal format of the name so the message may be used to determine the real profile name that RACF attempted to locate.

VOLUME

An array of volume serial numbers for volumes containing the data set. Each volume is a 6-byte character field.

V

A 2-byte variable that contains a subscript to the volume array. V is initialized to -1.

VOLUME is not available for generic data set profiles and is not available from commands if the VOLUME keyword was not specified. An attempt to reference nonexistent volumes (subscript 0 or greater than the number of volumes in the VOLUME array) results in a VOLUME parameter which contains *BLANK as a character string.

If you reference VOLUME in an ICHNCONV SELECT macro without a subscript, RACF tests the condition for each volume in turn until the condition is true. The variable V is set to the subscript of the volume for which the condition was true. If the condition is not true, the subscript variable will be negative one (-1).

For all conditions except NE (not equal), the implied linkage is OR; for the NE condition, the implied linkage is AND. For example,

SELECT COND=(VOLUME,EQ,'ABC') means

SELECT COND=((VOLUME,1),EQ,'ABC',OR)
 SELECT COND=((VOLUME,2),EQ,'ABC',OR) ...

while

SELECT COND=(VOLUME,NE,'ABC') means

SELECT COND=((VOLUME,1),NE,'ABC',AND)
 SELECT COND=((VOLUME,2),NE,'ABC',AND) ...

You may use any numeric variable as a subscript for VOLUME. If VOLUME is in an ICHNCONV ACTION macro without a subscript, RACF uses the current value of V as the subscript.

VCT

A 2-byte binary field containing the number of volumes in the VOLUME array. If volume information is not available, VCT has a value of zero.

OLDVOL

A 6-byte character field containing the volume serial number of

ICHNCONV macro

the volume that the data set currently resides on. This field is available during a RACDEF ADDVOL or RACDEF CHGVOL request.

WKX, WKY, WKZ

These are 2-byte binary fields that may be used as temporary work variables to save subscripts and other numeric data within and between conventions.

WKA, WKB, WKC

These are 8-byte character fields that may be used as temporary work variables to save qualifiers and other non-numeric data within and between conventions.

RACUID

The caller's user ID.

Note: If naming convention table processing is invoked from an environment where no ACEE is present to define the current user, a default value of * is used for RACUID.

RACGPID

The caller's current connect group.

Note: If naming convention table processing is invoked from an environment where no ACEE is present to define the current user, a default value of * is used for RACGPID.

RACUID3

The user ID used for third-party RACHECK.

RACGPID3

The group used for third-party RACHECK

Note: For RACROUTE REQUEST=AUTH (event code X'0100'):

- RACUID and RACGPID are the user and group used for non-third-party authorization checking. They are acquired from an address space level ACEE, a task level ACEE, or the ACEE= parameter on the RACROUTE REQUEST macro.
- RACUID3 and RACGPID3 are used for third-party authorization checking. They contain blanks for all other event codes. If the REQUEST=AUTH specifies a GROUP and no USERID, RACUID3 is *NONE*. If USERID is specified and no GROUP, RACGPID3 is blanks. RACUID3 and RACGPID3 might not contain a valid user or group. Their values are obtained from the RACROUTE REQUEST=AUTH parameters and have not been validated by RACF at the time the naming convention was called.

operator

Specifies the conditional operator: Valid operators are:

EQ Equal
GT Greater than
LT Less than
GE Greater than or equal
LE Less than or equal
NE Not equal

operand

Specifies a variable, a literal, or one of the following special symbols for use with the NAMETYPE variable:

- USER

- GROUP
- UNKNOWN

The operand used should match the length and type of the variable. If the length does not match, RACF performs padding or truncation in the normal manner. If the type does not match, the results are unpredictable.

If operand is specified as a literal, it can be:

- A character string enclosed in quotes
- A decimal number
- A hexadecimal string in the form X'string'

ICHNCONV ACTION

An ICHNCONV ACTION macro changes the value of variables. Use these macros to convert the data set name to the standard RACF format. RACF processes the ACTION macros in sequence.

The format of the ICHNCONV ACTION macro is:

```
[label] ICHNCONV ACTION,SET=(variable,value)
```

ACTION

Identifies a naming convention action. You can code multiple ICHNCONV ACTION macros.

SET=(variable,value)

Changes the qualifiers of a data set name and other variables.

variable

Specifies the variables that the convention can reference and set. See the preceding description of ICHNCONV SELECT for a description of these variables.

The following variables can be set:

- UQ
- QUAL
- G
- U
- V
- NAMETYPE
- WKA, WKB, WKC
- WKX, WKY, WKZ

value

Specifies the value given to the variable. Value can be another variable, a literal, or one of the following special symbols for use with the NAMETYPE variable:

- USER
- GROUP
- UNKNOWN

The value assigned to a variable should match the length and type of the variable. If the length does not match, RACF performs padding or truncation in the normal manner. If the type does not match, the results are unpredictable.

ICHNCONV macro

If you specify value as a variable, it can be any of the variables defined in the description of ICHNCONV SELECT.

If value is a literal, it can be:

- A character string enclosed in quotes
- A decimal number
- A hexadecimal string of the form X'string'

ICHNCONV END

An ICHNCONV END macro terminates the naming convention.

The format of the ICHNCONV END macro is:

```
[label] ICHNCONV END,NEXT=(convention name|'SUCCESS'|'NEXT'|'ERROR')
```

END

Identifies the end of the naming convention. Each convention must have one ICHNCONV END.

NEXT= (convention name|'SUCCESS'|'NEXT'|'ERROR')

Specifies where control goes after this convention executes, if the conditions specified in the ICHNCONV SELECT macros have been met or if there are no ICHNCONV SELECT macros in this convention.

If NEXT=convention name, processing continues with the specified convention and skips intervening conventions in the table. The specified convention must not precede the current convention in the table; otherwise, the RACF request fails.

If NEXT='NEXT', processing continues with the next convention in sequence. If NEXT='NEXT' is coded or defaulted to on the last convention in the table, processing is the same as if NEXT='SUCCESS' was coded.

If NEXT='SUCCESS', then the convention processing routine bypasses further convention processing and returns "a successful name processing" return code to the RACF routine that called it. The RACF routine will continue to process normally using the name returned by the convention processing routine.

If NEXT='ERROR', then the convention processing routine bypasses further processing and returns "an invalid data set name" return code to the RACF routine that called it. The RACF routine will terminate processing and fail the request.

ICHNCONV FINAL

An ICHNCONV FINAL macro terminates the naming convention table. (The naming convention table has one ICHNCONV FINAL macro.)

The format of the ICHNCONV FINAL macro is:

```
[label] ICHNCONV FINAL
```

FINAL

Identifies the end of the naming conventions table. There must be only one ICHNCONV FINAL macro in the table and it must be the last entry in the table.

Example of a Naming Convention Table

The following example of a naming convention table illustrates some ways that a table could be coded.

The first convention checks for data sets that are already in the correct RACF format, with a user ID or group name in the high-level qualifier or system data sets that start with the characters SYS. This convention bypasses all further checks because no further changes are needed.

```
ICHNCONV DEFINE,NAME=CHECK1
ICHNCONV SELECT,COND=((GQ,1),EQ,RACUID,OR)
ICHNCONV SELECT,COND=((GQ,1),EQ,RACGPID,OR)
ICHNCONV SELECT,COND=((GQ,1,1,3),EQ,'SYS')
ICHNCONV END,NEXT='SUCCESS'
```

This convention checks for data set names that have three or more qualifiers and any qualifier is the user's ID. The user ID is moved to the start of the name and deleted from its current position. ICHNCONV sets the type indicator and processing continues with convention CHECK4.

```
ICHNCONV DEFINE,NAME=CHECK2
ICHNCONV SELECT,COND=(QCT,GE,3,AND)
ICHNCONV SELECT,COND=(GQ,EQ,RACUID)
ICHNCONV ACTION,SET=(NAMETYPE,USER)
ICHNCONV ACTION,SET=((UQ,0),(GQ,G))
ICHNCONV ACTION,SET=((UQ,G),' ')
ICHNCONV END,NEXT=CHECK4
```

For all data sets that did not pass the first two conventions the first four characters of the third and fourth qualifiers are concatenated to form a new fifth qualifier. The user's current connect group becomes a high-level qualifier. Processing continues (by default) with the next convention.

```
ICHNCONV DEFINE,NAME=CHECK3
ICHNCONV ACTION,SET=((UQ,0),RACGPID)
ICHNCONV ACTION,SET=((UQ,5,1,4),(GQ,3,1,4))
ICHNCONV ACTION,SET=((UQ,5,5,8),(GQ,4,1,4))
ICHNCONV ACTION,SET=(NAMETYPE,GROUP)
ICHNCONV END
```

The installation has decided to enforce a standard that all three-qualifier data set names must have a data set type code as the last qualifier. Any qualifiers that are not in the list will cause the name to be rejected.

```
ICHNCONV DEFINE,NAME=CHECK4
ICHNCONV SELECT,COND=(QCT,EQ,3,AND)
ICHNCONV SELECT,COND=((GQ,3),NE,'PLI',AND)
ICHNCONV SELECT,COND=((GQ,3),NE,'DATA',AND)
ICHNCONV SELECT,COND=((GQ,3),NE,'COBOL',AND)
ICHNCONV SELECT,COND=((GQ,3),NE,'ASM')
ICHNCONV END,NEXT='ERROR'
```

The ICHNCONV FINAL macro terminates the table. An Assembler END statement is necessary to terminate the assembly.

ICHNCONV macro

```
ICHNCONV FINAL
END
```

ICHRFRTB Macro

The ICHRFRTB macro generates entries in the RACF router table. This table controls the action taken by the RACF router ICHRFRO0 when invoked by the RACROUTE macro. The router table has two parts. IBM supplies module ICHRFROX, which must not be modified. The installation optionally supplies module ICHRFRO1 so you can add entries for locally defined resource classes or requestor/subsystem combinations.

The ICHRFROX module supplied by IBM contains one entry for each entry in the class descriptor table, plus one entry for each of the DATASET, USER, GROUP, and CONNECT classes. For all entries, the operands REQSTOR and SUBSYS have the default value (all blanks), and the ACTION operand is set to RACF. In addition, several special entries related to program control and tape data set support are present. These entries also have non-blank REQSTOR and SUBSYS values.

Before adding a user-defined entry to the class descriptor table, a corresponding entry must be present in the RACF router table. The RACF router table entries are made as follows:

1. If the class has RACLIST=ALLOWED, use ICHRFRTB to create a router table entry. Code the ICHRFRTB macro with ACTION=RACF and specify blanks for both the REQSTOR= and the SUBSYS= parameters so that RACF can process the class if you issue a SETROPTS RACLIST command.
2. If your application uses RACROUTE, and requires REQSTOR= and SUBSYS=, you will need to code an additional ICHRFRTB macro specifying ACTION=RACF and the appropriate requester and subsystem values.

ICHRFRTB concatenates the values specified for the REQSTOR, SUBSYS, and CLASS operands to form a 24-character string defining the entry. The macro matches these values against the string formed by the values specified on the RACROUTE macro instruction.

The ICHRFRTB macro definition is as follows:

```
[label] ICHRFRTB [ACTION=NONE|RACF]
                [,CLASS=classname]
                [,REQSTOR=requestor-name]
                [,SUBSYS=subsystem-name]
                [TYPE=END]
```

ACTION=

Specifies the action to be taken for this entry. This operand is required unless TYPE=END is specified.

NONE Specifies that no action is to be taken for this entry.

RACF Specifies that RACF is to be called for this entry.

CLASS=class name

specifies the name of the resource class. You must use the same name that is specified in the corresponding class descriptor table entry. This operand is required unless TYPE=END is specified.

REQSTOR=requestor-name

Specifies the 8-character name to be used, along with CLASS and SUBSYS, to form the 24-character string defining the entry. Installations should begin

requestor names with a # (X'7B'), @ (X'7C') or \$ (X'5B'), because requestor names supplied by IBM do not begin with those characters. If you do not specify a requestor name, the default is a string of 8 blanks. If you code REQSTOR, you should also code the CLASS operand.

SUBSYS=subsystem-name

Specifies the 8-character name to be used, along with CLASS and REQSTOR, to form the 24-character string defining the entry. Installations should begin subsystem names with a # (X'7B'), @ (X'7C') or \$ (X'5B'), because subsystem names supplied by IBM will not begin with such characters. If no subsystem name is specified, it defaults to a string of 8 blanks. This operand should not be coded unless CLASS is also specified.

TYPE=END

Indicates the end of the ICHRR01 table. You must code TYPE=END on the last ICHRFRTB macro instruction. If TYPE=END is specified, no other operands can be coded.

The RACF Router Table Supplied by IBM (ICHRFR0X)

```

ICHRFRTB CLASS=DATASET, ACTION=RACF
ICHRFRTB CLASS=USER, ACTION=RACF
ICHRFRTB CLASS=GROUP, ACTION=RACF
ICHRFRTB CLASS=CONNECT, ACTION=RACF
ICHRFRTB CLASS=DASDVOL, ACTION=RACF
ICHRFRTB CLASS=GDASDVOL, ACTION=RACF
ICHRFRTB CLASS=TAPEVOL, ACTION=RACF
ICHRFRTB CLASS=TERMINAL, ACTION=RACF
ICHRFRTB CLASS=GTERMINL, ACTION=RACF
ICHRFRTB CLASS=APPL, ACTION=RACF
ICHRFRTB CLASS=TIMS, ACTION=RACF
ICHRFRTB CLASS=GIMS, ACTION=RACF
ICHRFRTB CLASS=AIMS, ACTION=RACF
ICHRFRTB CLASS=TCICSTRN, ACTION=RACF
ICHRFRTB CLASS=GCICSTRN, ACTION=RACF
ICHRFRTB CLASS=PCICSPSB, ACTION=RACF
ICHRFRTB CLASS=QCICSPSB, ACTION=RACF
ICHRFRTB CLASS=GMBR, ACTION=RACF
ICHRFRTB CLASS=GLOBAL, ACTION=RACF
ICHRFRTB CLASS=DSNR, ACTION=RACF
ICHRFRTB CLASS=FACILITY, ACTION=RACF
ICHRFRTB CLASS=SCDMBR, ACTION=RACF
ICHRFRTB CLASS=SECDATA, ACTION=RACF
ICHRFRTB CLASS=FCICSFCT, ACTION=RACF
ICHRFRTB CLASS=HCICSFCT, ACTION=RACF
ICHRFRTB CLASS=JCICSJCT, ACTION=RACF
ICHRFRTB CLASS=KCICSJCT, ACTION=RACF
ICHRFRTB CLASS=DCICSDCT, ACTION=RACF
ICHRFRTB CLASS=ECICSDCT, ACTION=RACF
ICHRFRTB CLASS=SCICSTST, ACTION=RACF
ICHRFRTB CLASS=UCICSTST, ACTION=RACF
ICHRFRTB CLASS=MCICSPPT, ACTION=RACF
ICHRFRTB CLASS=NCICSPPT, ACTION=RACF
ICHRFRTB CLASS=ACICSPCT, ACTION=RACF
ICHRFRTB CLASS=BCICSPCT, ACTION=RACF
ICHRFRTB CLASS=PMBR, ACTION=RACF
ICHRFRTB CLASS=PROGRAM, ACTION=RACF
ICHRFRTB CLASS=DATASET, REQSTOR=CLOSE, SUBSYS=OCEOV, ACTION=RACF
ICHRFRTB CLASS=DATASET, REQSTOR=TAPEOPEN, SUBSYS=OCEOV, ACTION=RACF
ICHRFRTB CLASS=DATASET, REQSTOR=TAPERST, SUBSYS=RESTART, ACTION=RACF
ICHRFRTB CLASS=TAPEVOL, REQSTOR=TAPEOPEN, SUBSYS=OCEOV, ACTION=RACF
ICHRFRTB CLASS=TSOPROC, ACTION=RACF
ICHRFRTB CLASS=ACCTNUM, ACTION=RACF
ICHRFRTB CLASS=PERFGRP, ACTION=RACF
ICHRFRTB CLASS=TSOAUTH, ACTION=RACF

```

ICHRFRTB macro

ICHRFRTB CLASS=DATASET,REQSTOR=TAPEEOV,SUBSYS=OCEOV,ACTION=RACF
ICHRFRTB CLASS=TAPEVOL,REQSTOR=TAPEEOV,SUBSYS=OCEOV,ACTION=RACF
ICHRFRTB CLASS=VMCMD,ACTION=RACF
ICHRFRTB CLASS=VMNODE,ACTION=RACF
ICHRFRTB CLASS=VMBATCH,ACTION=RACF
ICHRFRTB CLASS=FIELD,ACTION=RACF
ICHRFRTB CLASS=PROPCNTL,ACTION=RACF
ICHRFRTB CLASS=PROPCNTL,REQSTOR=PROPCHK,SUBSYS=IEFCMAUT,ACTION=RACF
ICHRFRTB CLASS=MGMTCLAS,ACTION=RACF
ICHRFRTB CLASS=STORCLAS,ACTION=RACF
ICHRFRTB CLASS=FACILITY,REQSTOR=ABDUMP,SUBSYS=ABDUMP,ACTION=RACF
ICHRFRTB CLASS=VMBR,ACTION=RACF
ICHRFRTB CLASS=VMEVENT,ACTION=RACF
ICHRFRTB CLASS=VMXBR,ACTION=RACF
ICHRFRTB CLASS=VMXEVENT,ACTION=RACF
ICHRFRTB CLASS=VMDISK,ACTION=RACF
ICHRFRTB CLASS=VMRDR,ACTION=RACF
ICHRFRTB CLASS=APPCLU,ACTION=RACF
ICHRFRTB CLASS=SECLABEL,ACTION=RACF
ICHRFRTB CLASS=SMESSAGE,ACTION=RACF
ICHRFRTB CLASS=DEVICES,ACTION=RACF
ICHRFRTB CLASS=VTAMAPPL,ACTION=RACF
ICHRFRTB CLASS=PSFMPL,ACTION=RACF
ICHRFRTB CLASS=OPERCMDs,ACTION=RACF
ICHRFRTB CLASS=WRITER,ACTION=RACF
ICHRFRTB CLASS=JESSPOOL,ACTION=RACF
ICHRFRTB CLASS=JESJOBS,ACTION=RACF
ICHRFRTB CLASS=JESINPUT,ACTION=RACF
ICHRFRTB CLASS=CONSOLE,ACTION=RACF
ICHRFRTB CLASS=TEMPDSN,ACTION=RACF
ICHRFRTB CLASS=DIRAUTH,ACTION=RACF
ICHRFRTB CLASS=SURROGAT,ACTION=RACF
ICHRFRTB CLASS=NODES,ACTION=RACF
ICHRFRTB CLASS=NODMBR,ACTION=RACF
ICHRFRTB CLASS=RVARSMBR,ACTION=RACF
ICHRFRTB CLASS=RACFVARS,ACTION=RACF
ICHRFRTB CLASS=DIRECTRY,ACTION=RACF
ICHRFRTB CLASS=FILE,ACTION=RACF
ICHRFRTB CLASS=CIMS,ACTION=RACF
ICHRFRTB CLASS=DIMS,ACTION=RACF
ICHRFRTB CLASS=DLFCLASS,ACTION=RACF
ICHRFRTB CLASS=CCICSCMD,ACTION=RACF
ICHRFRTB CLASS=VCICSCMD,ACTION=RACF
ICHRFRTB CLASS=PIMS,ACTION=RACF
ICHRFRTB CLASS=QIMS,ACTION=RACF
ICHRFRTB CLASS=SIMS,ACTION=RACF
ICHRFRTB CLASS=UIMS,ACTION=RACF
ICHRFRTB CLASS=FIMS,ACTION=RACF
ICHRFRTB CLASS=HIMS,ACTION=RACF
ICHRFRTB CLASS=OIMS,ACTION=RACF
ICHRFRTB CLASS=WIMS,ACTION=RACF
ICHRFRTB CLASS=VMMAC,ACTION=RACF
ICHRFRTB CLASS=VMSEGMT,ACTION=RACF
ICHRFRTB CLASS=SFSCMD,ACTION=RACF
ICHRFRTB CLASS=SDSF,ACTION=RACF
ICHRFRTB CLASS=GSDFS,ACTION=RACF
ICHRFRTB CLASS=APPCTP,ACTION=RACF
ICHRFRTB CLASS=APPCSI,ACTION=RACF
ICHRFRTB CLASS=APPCPORT,ACTION=RACF
ICHRFRTB CLASS=CSFSERV,ACTION=RACF
ICHRFRTB CLASS=CSFKEYS,ACTION=RACF
ICHRFRTB CLASS=GCSFKEYS,ACTION=RACF
ICHRFRTB CLASS=NVASAPDT,ACTION=RACF
ICHRFRTB CLASS=PROGRAM,REQSTOR=FAE,SUBSYS=CONTENTS,ACTION=RACF
ICHRFRTB CLASS=PROGRAM,REQSTOR=PROGMCHK,SUBSYS=CONTENTS,ACTION=RACF
ICHRFRTB CLASS=USER,REQSTOR=FMH5-MGR,SUBSYS=APPC/MVS,ACTION=RACF
ICHRFRTB CLASS=USER,REQSTOR=VTAMEXIT,SUBSYS=APPC/MVS,ACTION=RACF

ICHRFRTB CLASS=USER,REQSTOR=SIGNONTP,SUBSYS=APPC/MVS,ACTION=RACF
 ICHRFRTB CLASS=USER,REQSTOR=APPCSCH,SUBSYS=APPC/MVS,ACTION=RACF
 ICHRFRTB CLASS=APPCTP,REQSTOR=APPCSDFM,SUBSYS=APPC/MVS,ACTION=RACF
 ICHRFRTB CLASS=APPCSI,REQSTOR=APPCSDFM,SUBSYS=APPC/MVS,ACTION=RACF
 ICHRFRTB CLASS=FACILITY,REQSTOR=APPCSDFM,SUBSYS=APPC/MVS,ACTION=RACF
 ICHRFRTB CLASS=RMTOPS,ACTION=RACF
 ICHRFRTB CLASS=PROGRAM,REQSTOR=PADSCHK,SUBSYS=CONTENTS,ACTION=RACF
 ICHRFRTB CLASS=INFOMAN,ACTION=RACF
 ICHRFRTB CLASS=GINFOMAN,ACTION=RACF
 ICHRFRTB CLASS=APPCSERV,ACTION=RACF
 ICHRFRTB CLASS=APPCSERV,REQSTOR=APPCSDFM,SUBSYS=APPC/MVS,ACTION=RACF
 ICHRFRTB CLASS=DIRSRCH,ACTION=RACF
 ICHRFRTB CLASS=DIRACC,ACTION=RACF
 ICHRFRTB CLASS=FSOBJ,ACTION=RACF
 ICHRFRTB CLASS=FSSEC,ACTION=RACF
 ICHRFRTB CLASS=PROCESS,ACTION=RACF
 ICHRFRTB CLASS=PROCACT,ACTION=RACF
 ICHRFRTB CLASS=RACGLIST,ACTION=RACF
 ICHRFRTB CLASS=LFSCCLASS,ACTION=RACF
 ICHRFRTB CLASS=RODMMGR,ACTION=RACF
 ICHRFRTB CLASS=MQQUEUE,ACTION=RACF
 ICHRFRTB CLASS=GMQUEUE,ACTION=RACF
 ICHRFRTB CLASS=MQPROC,ACTION=RACF
 ICHRFRTB CLASS=GMQPROC,ACTION=RACF
 ICHRFRTB CLASS=MQNLIST,ACTION=RACF
 ICHRFRTB CLASS=GMQNLIST,ACTION=RACF
 ICHRFRTB CLASS=MQADMIN,ACTION=RACF
 ICHRFRTB CLASS=GMQADMIN,ACTION=RACF
 ICHRFRTB CLASS=MQCMDS,ACTION=RACF
 ICHRFRTB CLASS=MQCONN,ACTION=RACF
 ICHRFRTB CLASS=SUBSYSNM,ACTION=RACF
 ICHRFRTB CLASS=NETSPAN,ACTION=RACF
 ICHRFRTB CLASS=NETCMDS,ACTION=RACF
 ICHRFRTB CLASS=CPSMOBJ,ACTION=RACF
 ICHRFRTB CLASS=GCPSMOBJ,ACTION=RACF
 ICHRFRTB CLASS=CPSMXMP,ACTION=RACF
 ICHRFRTB CLASS=PTKTDATA,ACTION=RACF
 ICHRFRTB CLASS=STARTED,ACTION=RACF
 ICHRFRTB CLASS=MQCHAN,ACTION=RACF
 ICHRFRTB CLASS=GMQCHAN,ACTION=RACF
 ICHRFRTB CLASS=DBNFORM,ACTION=RACF
 ICHRFRTB CLASS=IBMOPC,ACTION=RACF
 ICHRFRTB CLASS=LOGSTRM,ACTION=RACF
 ICHRFRTB CLASS=PTKTVAL,ACTION=RACF
 ICHRFRTB CLASS=RRSFDATA,ACTION=RACF
 ICHRFRTB CLASS=IPCOBJ,ACTION=RACF
 ICHRFRTB CLASS=SYSMVIEW,ACTION=RACF
 ICHRFRTB CLASS=KEYSMSTR,ACTION=RACF
 ICHRFRTB CLASS=DCEUUIDS,ACTION=RACF
 ICHRFRTB CLASS=CBIND,ACTION=RACF
 ICHRFRTB CLASS=SERVER,ACTION=RACF
 ICHRFRTB CLASS=SOMDOBJs,ACTION=RACF
 ICHRFRTB CLASS=VMPOSIX,ACTION=RACF
 ICHRFRTB CLASS=ALCSAUTH,ACTION=RACF
 ICHRFRTB CLASS=GSOMDOBJ,ACTION=RACF
 ICHRFRTB CLASS=TMEADMIN,ACTION=RACF
 ICHRFRTB CLASS=DSNADM,ACTION=RACF
 ICHRFRTB CLASS=GDSNBP,ACTION=RACF
 ICHRFRTB CLASS=GDSNCL,ACTION=RACF
 ICHRFRTB CLASS=GDSNDB,ACTION=RACF
 ICHRFRTB CLASS=GDSNPK,ACTION=RACF
 ICHRFRTB CLASS=GDSNPN,ACTION=RACF
 ICHRFRTB CLASS=GDSNSG,ACTION=RACF
 ICHRFRTB CLASS=GDSNSM,ACTION=RACF
 ICHRFRTB CLASS=GDSNTB,ACTION=RACF
 ICHRFRTB CLASS=GDSNTS,ACTION=RACF
 ICHRFRTB CLASS=MDSNBP,ACTION=RACF

ICHRFRTB macro

```
ICHRFRTB CLASS=MDSNCL, ACTION=RACF
ICHRFRTB CLASS=MDSNDB, ACTION=RACF
ICHRFRTB CLASS=MDSNPK, ACTION=RACF
ICHRFRTB CLASS=MDSNPB, ACTION=RACF
ICHRFRTB CLASS=MDSNSG, ACTION=RACF
ICHRFRTB CLASS=MDSNSM, ACTION=RACF
ICHRFRTB CLASS=MDSNTB, ACTION=RACF
ICHRFRTB CLASS=MDSNTS, ACTION=RACF
ICHRFRTB CLASS=PROGRAM, REQSTOR=CKPGMDSN, SUBSYS=CONTENTS, ACTION=RACF
ICHRFRTB CLASS=DIGTCERT, ACTION=RACF
ICHRFRTB CLASS=ROLE, ACTION=RACF
ICHRFRTB CLASS=UNIXMAP, ACTION=RACF
ICHRFRTB CLASS=NOTELINK, ACTION=RACF
ICHRFRTB CLASS=NDLINK, ACTION=RACF
ICHRFRTB CLASS=DIGTRING, ACTION=RACF
ICHRFRTB CLASS=UNIXPRIV, ACTION=RACF
ICHRFRTB CLASS=JAVA, ACTION=RACF
ICHRFRTB CLASS=SERVAUTH, ACTION=RACF
ICHRFRTB CLASS=MDSNUT, ACTION=RACF
ICHRFRTB CLASS=GDSNUT, ACTION=RACF
ICHRFRTB CLASS=MDSNUF, ACTION=RACF
ICHRFRTB CLASS=GDSNUF, ACTION=RACF
ICHRFRTB CLASS=MDSNSC, ACTION=RACF
ICHRFRTB CLASS=GDSNSC, ACTION=RACF
ICHRFRTB CLASS=MDSNSP, ACTION=RACF
ICHRFRTB CLASS=GDSNSP, ACTION=RACF
ICHRFRTB CLASS=DIGTNMAP, ACTION=RACF
ICHRFRTB CLASS=DIGTCRIT, ACTION=RACF
ICHRFRTB CLASS=REALM, ACTION=RACF
ICHRFRTB CLASS=KERBLINK, ACTION=RACF
ICHRFRTB CLASS=ILMADMIN, ACTION=RACF
ICHRFRTB CLASS=EJBROLE, ACTION=RACF
ICHRFRTB CLASS=GEJBROLE, ACTION=RACF
ICHRFRTB CLASS=MDSNJR, ACTION=RACF
ICHRFRTB CLASS=GDSNJR, ACTION=RACF
ICHRFRTB CLASS=CACHECLS, ACTION=RACF
```

Chapter 2. Panel Driver Interface

Installations can implement a panel driver interface between an application program and the RACF panels. In order to use the panel driver interface, the programmer who writes the interface should be familiar with TSO CLIST or ISPF programming techniques.

Invoking the Panel Driver Interface

When you invoke the panel driver interface module (ICHSPF03), your program must pass it the following three parameters as ISPF variables:

- ICHFUNCT** the type of function that ICHSPF03 is to perform: you may specify blank, ADD, CHG, DEL, ACC, and DSP.
- ICHRESCL** the name of the resource class: for example; group, user, data set, or any of the general resource classes defined to RACF in the class descriptor table (CDT). The classes supplied by IBM are in Appendix C, "IBM-supplied class descriptor table entries" on page 351. Other classes can be added by your installation.
- ICHRESNM** a resource name within the resource class, supplied in conjunction with the resource class by the programmer writing the interface.

These parameters are passed to ICHSPF03 using the ISPLINK SELECT service and the function variable pool.

ICHSPF03 matches the first two arguments passed in the parameter list (function and resource class) to the panel mapping table to determine which RACF panel to display.

Panel Mapping Table

Function	Resource Class	Panel ID
bbb	bbbbbbbb	ICHP00
bbb	DATASET	ICHP10
ADD	DATASET	ICHP11
CHG	DATASET	ICHP12
DEL	DATASET	ICHP13
ACC	DATASET	ICHP14
DSP	DATASET	ICHP18
bbb	general	ICHP20
ADD	general	ICHP21
CHG	general	ICHP22
DEL	general	ICHP23
ACC	general	ICHP24
DSP	general	ICHP28
bbb	GROUP	ICHP30
ADD	GROUP	ICHP31
CHG	GROUP	ICHP32
DEL	GROUP	ICHP33
DSP	GROUP	ICHP38
bbb	USERID	ICHP40
ADD	USERID	ICHP41
CHG	USERID	ICHP42
DEL	USERID	ICHP43

ICHSPF03

Function	Resource Class	Panel ID
DSP	USERID	ICHP48

Notes:

1. In the table above, 'general' stands for any valid general resource class.
2. bbb... represents blanks.

If the caller enters a *resource* class that is not defined in the table, the argument defaults to general. If the caller enters a *function* that is not defined in the table, ICHSPF03 issues an error message.

ICHSPF03 issues a VREPLACE within the panel driver interface to update the shared variable pool with the parameters passed from the user's function panel. ICHSPF03 then places those parameters in the panels where variables are required to identify the resource. Thus, the user does not have to constantly retype parameters. If there is an error in the caller's parameter list, ICHSPF03 issues an error message.

The ISPLINK Call

The following is an example of a declare for the RACF panel driver interface:

```
DCL Buffer Char(13) Init('PGM(ICHSPF03)');
```

The following is the format of a call to the RACF panel driver interface:

```
CALL ISPLINK(SELECT, LENGTH(BUFFER), BUFFER)
```

ICHSPF03 issues an ISPLINK call for the target RACF panel. Upon return from the RACF panel after performing the requested function, RACF enters a return code in Register 15.

The return code will be one of the following:

- 0 = successful completion of the function
- 12 = invalid function code specified
- 16 = variable not defined in the function pool

The way in which ICHSPF03 invokes the RACF panels depends on the way the programmer coded the interface. For example, if the parameters passed were ICHFUNCT = bbb, ICHRESCL = DATASET, and ICHRESNM = A.B.C, then ICHP10 will be displayed as:

```
PROFILE NAME === >A.B.C
```

Note: On this screen, you can modify the profile name.

If the parameters passed were ICHFUNCT = CHG, ICHRESCL = DASDVOL, and ICHRESNM = DPT67V, then ICHP22 will be displayed as:

```
CLASS: DASDVOLPROFILE NAME: DPT67V
```

Note: In this case, you cannot modify the class or the profile name.

Example of a RACF Panel Interface Coding Sequence

The following is an example of a user-written coding sequence to create an interface to the RACF panels. You can also call the interface from a CLIST in a similar fashion.

```
/*Create Variables in the Function Variable Pool*/  
Call ISPLINK(VDEFINE,'ICHFUNCT',ICHFUNCT,'CHAR',LENGTH(ICHFUNCT));  
Call ISPLINK(VDEFINE,'ICHRESCL',ICHRESCL,'CHAR',LENGTH(ICHRESCL));  
Call  
ISPLINK(VDEFINE,'ICHRESNM',ICHRESNM,'CHAR',LENGTH(ICHRESNM));  
/*Copy variables from Function Pool to Shared Variable Pool*/  
Call ISPLINK('VPUT','ICHFUNCT');  
Call ISPLINK('VPUT','ICHRESCL');  
Call ISPLINK('VPUT','ICHRESNM');  
/*Call the Panel Driver Interface*/  
Call ISPLINK(SELECT,LENGTH(BUFFER),BUFFER);  
/*Test return code from the PDI for possible errors */
```

ICHSPF03

Chapter 3. Profile Name List Service Routine

RACF provides installations with a profile name list service routine (IRRPNL00) that allows TSO or other programs to call RACF to retrieve the names of profiles within a class that a given user ID can access at READ level or higher.

To perform this function, IRRPNL00 searches the RACF class descriptor table (CDT) for the class name. If the class is found and the class has been processed by SETROPTS RACLIST, IRRPNL00 checks each profile name processed by SETROPTS RACLIST to see if the specified user ID is authorized to access the profile at READ level or higher. When IRRPNL00 finds a match, it places the profile name into the input work area.

IRRPNL00 begins its search with the first profile and continues its search until it checks all the profiles or until the size of the list exceeds the size of the work area.

IRRPNL00 resides in LPA. RACF loads the address of IRRPNL00 into RCVTPNL0 during RACF initialization. The caller of IRRPNL00 may use the address in RCVTPNL0.

Notes:

1. To use the profile name list service routine, you must ensure that a SETROPTS RACLIST has been issued for each class name you intend to search.
2. Your program is responsible for obtaining and releasing the storage which IRRPNL00 uses to store the profile name list.
3. Callers of IRRPNL00 must be running in Key 0, task mode, with no locks held, and in 31-bit mode addressing.

Invoking the Profile Name List Service Routine

When you invoke the profile name list service routine, (IRRPNL00), your program must pass it the following four parameters:

Classname an 8-character class name from which RACF derives the profile names to which the user ID has authorization

Work area length

a fullword that contains the length of the area in which IRRPNL00 is going to build the profile name list

Work Area

a fullword pointer that contains the address of the work area where IRRPNL00 is going to build the profile name list

ACEE pointer

a fullword pointer that contains the address of the ACEE for the user ID for whom profile authorization is being determined

Note: If the ACEE pointer is zero, IRRPNL00 uses the ACEE pointed to by TCBSENV.

If the TCBSENV pointer is zero, IRRPNL00 attempts to use the ASXBSENV field.

If the ASXBSENV field is zero, IRRPNL00 returns an error return code and reason code.

IRRPNL00

The calling program passes these parameters to IRRPNL00 using the CALL command.

If IRRPNL00 is being called by a RACF exit, it must be invoked using the SYNCH macro. See *z/OS MVS Programming: Assembler Services Guide*.

Format of Returned Profile Name List

A FIXED(31) count field which precedes the profile name list contains the total count of profile names returned by IRRPNL00. The format of the profile name list when it is placed in the work area is as follows:

NAME LENGTH	A 2-byte length of the profile name
FLAGS	A 1-byte flag field (only first bit used)
PROFILE NAME	A variable-length profile name

Note: The first bit of the flag field byte is on if the profile is a generic profile.

Return Codes

The return codes from IRRPNL00 follow RACF conventions with a return code of 0 indicating a successful search. The return codes are as follows:

Note to Reader

All return and reason codes are shown in hexadecimal.

The following return codes are returned in register 15, and the reason codes in register 0.

Return Code	Meaning
00	The Profile Name List function completed successfully.
04	No profiles found for which user ID had at least read access.
08	No profile entries found for that class. Indicates that either no profiles existed for the input class or the input class was not processed by SETROPTS RACLIST.
0C	The work area was not large enough to hold all the profile names.
14	Profile Name List parameter error
	Reason Code Meaning
	04 No ACEE available.
	08 Work Area too small to contain a single profile.
	10 Input Class name not valid.
18	Unable to establish ESTAE environment.
1C	Non-zero return code from the data space search routine: Return Code and Reason Codes are returned in the low-order and high-order half words of Register 0. Most are internal RACF codes indicating an error in RACF, except for the following:
	Reason Code Meaning
	00080008 Class not processed by SETROPTS RACLIST

00080018 RACLIST data space could not be accessed due to an ALESERV failure.

| **20**

ACEE has a default UTOKEN

| **24**

The ACEE UTOKEN has a port-of-entry calss indicated bit no port-of-entry name is supplied.

|

IRRPNL00

Chapter 4. Date Conversion Routine

RACF provides installations with the IRRDCR00 module, which is the date conversion routine that enables programs to specify and identify dates beyond the end of the 20th century.

Using this routine, installation and vendor applications can call RACF to convert a three-byte packed-decimal date to a four-byte packed-decimal date. The three-byte date has the form *yydddF*, and the four-byte date has the form *ccyydddF*, where *cc* is 00 for years 1971 through 1999 and is 01 for years 2000 through 2070. In the three-byte form, the routine interprets the year as 19 yy when yy is 71 or higher and as 20 yy when yy is less than 71.

This routine resides in the LPA. The system loads the address of this routine in RCVTDATP and sets bit RCVTD4OK (X'08') in flag byte RCVTMFLG during RACF initialization. The routine's caller can use the address in RCVTDATP.

Invoking the Date Conversion Routine

When a program invokes the date conversion routine, the program must pass two parameters to it:

Three-byte date	a three-byte field containing a packed-decimal date (format <i>yydddF</i>)
Four-byte date	a four-byte field

Note: This routine runs in the caller's mode, state, and key. Recovery is handled by the calling program.

Format of Returned Converted Date

The routine returns a four-byte packed-decimal date whose format is either *00yydddF* (for 1971-1999) or *01yydddF* (for 2000-2070).

If *ddd* is 000 in the three-byte *yydddF* date field passed to the routine, the routine returns 00 for *cc* (indicating a year 19 yy), regardless of what yy is.

Return Code

The return code from this routine follows RACF conventions with a return code of 00 (X'00') indicating successful date conversion. This code is sent to register 15.

The return code is as follows:

Note to Reader

The return code is shown in hexadecimal.
--

Return Code	Meaning
-------------	---------

00	The date conversion function completed successfully.
----	--

Date Conversion

Chapter 5. SMF Records

RACF produces three SMF records:

Type 80 Produced during RACF processing

Type 81 Produced at the completion of RACF initialization and the SETROPTS command

Type 83 Produced during RACF processing

The type 83 record is generated under the following circumstances: SETROPTS MLACTIVE is in effect and a RACF command (ADDSD, ALTDSD, DELDSD) has been issued that changed the security label of a data set profile.

The first 18 bytes of type 80 and 81 records represent the standard SMF header without subtypes. The first 24 bytes of type 83 records represent the standard SMF header with subtypes. See *z/OS MVS System Management Facilities (SMF)* for information about how to use SMF.

For sorting purposes, the RACF report writer reformats SMF records (types 20, 30, 80, 81 and 83) and uses these reformatted records as input to the modules that produce the RACF reports. There are two types of reformatted records - reformatted process records and reformatted status records. If you want to use the RACF report writer exit (ICHRSMFE) to produce additional reports or to add additional record selection criteria, you should familiarize yourself with the layouts of these reformatted records.

It is recommended that you use the RACROUTE system macro and its request types rather than the independent system macros. Table 1 shows each RACROUTE macro request type and the corresponding independent system macro.

Table 1. RACROUTE Request Types and Corresponding Independent RACF System Macro

RACROUTE Request Type	Independent RACF System Macro
REQUEST=AUTH	RACHECK
REQUEST=DEFINE	RACDEF
REQUEST=EXTRACT	RACXTRT
REQUEST=FASTAUTH	FRACHECK
REQUEST=LIST	RACLIST
REQUEST=STAT	RACSTAT
REQUEST=VERIFY	RACINIT
REQUEST=VERIFYX	RACINIT

Record Type 80: RACF Processing Record

RACF writes record type 80 for the following detected events:

- **Unauthorized attempts to enter the system.** For example, during RACF processing of a RACROUTE REQUEST=VERIFY macro instruction, RACF found that a RACF-defined user either (1) has supplied an invalid password, OI DCARD, or group name, (2) is not authorized access to the terminal, or (3) had insufficient security label authority.

SMF Records–Type 80

RACF always writes this violation record when it detects the unauthorized attempt; this violation record supplements the information that RACF sends to the security console in RACF message ICH408I.

- **Authorized attempts to enter the system.** RACF provides a RACROUTE REQUEST=VERIFY option to log successful signons and signoffs as well as ENVIR=CREATE or ENVIR=DELETE signons and signoffs. For the LOG keyword on the RACROUTE REQUEST=VERIFY macros, LOG=ALL or LOG=ASIS may be specified to control the generation of log records for RACROUTE REQUEST=VERIFY. The value of the LOG keyword is passed to both the RACROUTE REQUEST=VERIFY preprocessing and postprocessing installation exits. Both exits are invoked prior to the generation of a log record, and the LOG keyword value can be changed for both exits.
- **Authorized accesses or unauthorized attempts to access RACF-protected resources.** During RACF processing of a RACROUTE REQUEST=AUTH or REQUEST=DEFINE macro instruction, RACF found that one of the following events occurred:
 1. The user was permitted access to a RACF-protected resource and allowed to perform the requested operation.
 2. The user did not have sufficient access or group authority to access a RACF-protected resource, or supplied invalid data while attempting to perform an operation on a RACF-protected resource.

In the first case, RACF writes the record if the ALL or SUCCESS logging option is set in the resource profile by the ADDSD, ALTDSD, RALTER, or RDEFINE command and the access type is within the scope of the valid access types. RACF also writes the record if logging has been unconditionally requested by a RACROUTE REQUEST=AUTH postprocessing exit routine.

In the second case, RACF writes the violation record if the ALL or FAILURES logging option is set in the resource profile by the ADDSD, ALTDSD, RALTER, or RDEFINE command, or if logging is unconditionally requested by a RACROUTE REQUEST=AUTH postprocessing exit routine. The violation record supplements the information that RACF sends to the security console in RACF message ICH408I.

Note that the FAILURES (READ) option is the default in cases where new resources are RACF-protected.

For the preceding events, a RACROUTE REQUEST=AUTH exit routine can modify the logging options by changing the LOG parameter on a RACROUTE REQUEST=AUTH macro instruction from ASIS to NOFAIL, NONE, or NOSTAT, or by unconditionally requesting or suppressing logging with the logging control field. For information on the LOG parameter of a RACROUTE REQUEST=AUTH macro instruction, see *z/OS Security Server RACROUTE Macro Reference*. For information on the logging options of the ADDSD, ALTDSD, ALTUSER, RALTER, RDEFINE, and SETROPTS commands, see *z/OS Security Server RACF Command Language Reference*.

- **Authorized or unauthorized attempts to modify profiles on a RACF database.** During RACF command processing, RACF found that a user with the AUDITOR attribute specified that the following be logged:
 1. All detected changes to a RACF database by RACF commands or a RACROUTE REQUEST=DEFINE
 2. All RACF commands (except LISTDSD, LISTGRP, LISTUSER, RLIST, and SEARCH) issued by users with the SPECIAL attribute

3. All violations detected by RACF commands (except LISTGRP, LISTUSER, RLIST, and SEARCH)
4. Every RACROUTE REQUEST=AUTH and RACROUTE REQUEST=DEFINE issued for the user and all RACF commands (except LISTGRP, LISTUSER, RLIST and SEARCH) issued by the user

In the first three cases, RACF writes records if a user with the AUDITOR attribute specified AUDIT, SAUDIT, and CMDVIOL, respectively, on the SETROPTS command. In the fourth case, RACF writes the records if a user with the AUDITOR attribute specified UAUDIT on the ALTUSER command.

You can use SMF records to:

- Track the total use of a sensitive resource (if the ALL option is set)
- Identify the resources that are repeated targets of detected unauthorized attempts to access them (if the ALL or FAILURES option is set)
- Identify the users who make detected unauthorized requests
- Track SPECIAL user activity
- Track activity of a particular user

In most cases, RACF writes one record for each event. (RACF can write two records for one operation on a resource — for example, when a RACF-protected DASD data set is deleted with scratch.)

SMF record 80 contains the following information:

- The record type
- Time stamp (time and date)
- Processor identification
- Event code and qualifier (explained in Table 1)
- User identification
- Group name
- A count of the relocate sections
- Authorities used to successfully execute commands or access resources
- Reasons for logging
- Command processing error flag
- Foreground user terminal ID
- Foreground user terminal level number
- Job log number (job name, entry time, and date)
- RACF version, release and modification number
- SECLABEL of user

(The data in a relocate section is explained in “Table of Relocate Section Variable Data” on page 54 and “Table of Data Type 6 Command-Related Data” on page 67.)

The log record RACF creates is a standard type 80 SMF record.

The format of record type 80 is:

Offsets

Dec.	Hex.	Name	Length	Format	Description
0	0	SMF80LEN	2	Binary	Record length.
2	2	SMF80SEG	2	Binary	Segment descriptor.

SMF Records–Type 80

Offsets

Dec.	Hex.	Name	Length	Format	Description
4	4	SMF80FLG	1	Binary	System indicator Bit Meaning When Set 0-2 Reserved 3 MVS/SP Version 4 or 5 4 MVS/SP Version 3 5 MVS/SP Version 2 6 VS2 7 Reserved. Note: For MVS/SP Version 4, bits 3, 4, 5, and 6 will be on.
5	5	SMF80RTY	1	Binary	Record type: 80 (X'50').
6	6	SMF80TME	4	Binary	Time of day, in hundredths of a second, that the record was moved to the SMF buffer.
10	A	SMF80DTE	4	packed	Date that the record was moved to the SMF buffer, in the form <i>0ccyydddF</i> (where <i>F</i> is the sign).
14	E	SMF80SID	4	EBCDIC	System identification (from the SID parameter).
18	12	SMF80DES	2	Binary	Descriptor flags Bit Meaning When Set 0 The event is a violation 1 User is not defined to RACF 2 Record contains a version indicator (see SMF80VER) 3 The event is a warning 4 Record contains a version, release, and modification level number (see SMF80VRM) 5-15 Reserved.
20	14	SMF80EVT	1	Binary	Event code.
21	15	SMF80EVQ	1	Binary	Event code qualifier.
22	16	SMF80USR	8	EBCDIC	Identifier of the user associated with this event (jobname is used if the user is not defined to RACF).
30	1E	SMF80GRP	8	EBCDIC	Group to which the user was connected (stepname is used if the user is not defined to RACF).
38	26	SMF80REL	2	Binary	Offset to the first relocate section from the beginning of the record header (SMF80FLG).
40	28	SMF80CNT	2	Binary	Count of the number of relocate sections.
42	2A	SMF80ATH	1	Binary	Authorities used for processing commands or accessing resources Bit Meaning When Set 0 Normal authority check (resource access) 1 SPECIAL attribute (command processing) 2 OPERATIONS attribute (resource access, command processing) 3 AUDITOR attribute (command processing) 4 Installation exit processing (resource access) 5 Failsoft processing (resource access) 6 Bypassed-user ID = *BYPASS* (resource access) 7 Trusted attribute (resource access).

Offsets

Dec.	Hex.	Name	Length	Format	Description
43	2B	SMF80REA	1	Binary	Reason for logging. These flags indicate the reason RACF produced the SMF record Bit Meaning When Set 0 SETROPTS AUDIT(class)—changes to this class of profile are being audited. 1 User being audited 2 SPECIAL users being audited 3 Access to the resource is being audited due to the AUDIT option (specified when profile created or altered by a RACF command), a logging request from the RACROUTE REQUEST=AUTH exit routine, or because the operator granted access during failsoft processing. 4 RACROUTE REQUEST=VERIFY or initACEE failure. 5 This command is always audited 6 Violation detected in command and CMDVIOL is in effect 7 Access to entity being audited due to GLOBALAUDIT option.
44	2C	SMF80TLV	1	Binary	Terminal level number of foreground user (zero if not available).
45	2D	SMF80ERR	1	Binary	Command processing error flag Bit Meaning When Set 0 Command had error and RACF could not back out some changes 1 No profile updates were made because of error in RACF processing 2-7 Reserved.
46	2E	SMF80TRM	8	EBCDIC	Terminal ID of foreground user (zero if not available).
54	36	SMF80JBN	8	EBCDIC	Job name. For RACROUTE REQUEST=VERIFY records for batch jobs, this field can be zero.
62	3E	SMF80RST	4	Binary	Time, in hundredths of a second, that the reader recognized the JOB statement for this job. For RACROUTE REQUEST=VERIFY records for batch jobs, this field can be zero.
66	42	SMF80RSD	4	packed	Date the reader recognized the JOB statement for this job, in the form 0cyydddF (where F is the sign). For RACROUTE REQUEST=VERIFY records for batch jobs, this field can be zero.
70	46	SMF80UID	8	EBCDIC	User identification field from the SMF common exit parameter area. For RACROUTE REQUEST=VERIFY records for batch jobs, this field can be zero.
78	4E	SMF80VER	1	Binary	Version indicator (8 = Version 1, Release 8 or later). As of RACF 1.8.1, SMF80VRM is used instead.

SMF Records–Type 80

Offsets

Dec.	Hex.	Name	Length	Format	Description
79	4F	SMF80RE2	1	Binary	Additional reasons for logging
				Bit	Meaning When Set
				0	Security level control for auditing
				1	VMEVENT Auditing
				2	Class being audited due to SETROPTS LOGOPTIONS
				3	Entity audited due to SETROPTS SECLABELAUDIT
				4	Entity audited due to SETROPTS COMPATMODE
				5	Audited due to SETROPTS APPLAUDIT
				6	Audited because user not defined to z/OS UNIX
				7	Audited because user does not have appropriate authority for z/OS UNIX
80	50	SMF80VRM	4	EBCDIC	FMID for RACF
				2020	RACF 2.2 and OS/390 Security Server (RACF) V1 R2
				2030	OS/390 Security Server (RACF) V1 R3
				2040	OS/390 Security Server (RACF) V2 R4
				2060	OS/390 Security Server (RACF) V2 R6
				2608	OS/390 Security Server (RACF) V2 R8
				7703	OS/390 Security Server (RACF) V2 R10 and z/OS Security Server (RACF) V1 R1
				7705	z/OS Security Server (RACF) V1 R2
84	54	SMF80SEC	8	EBCDIC	Security label of the user.
92	5C	SMF80RL2	2	Binary	Offset to extended-length relocate sections.
94	5E	SMF80CT2	2	Binary	Count of extended-length relocate sections.
96	60	SMF80AU2	1	Binary	Authority used continued
				Bit	Meaning When Set
				0	z/OS UNIX superuser
				1	z/OS UNIX system function
				2-7	Reserved.
97	61	SMF80RSV	1	Binary	Reserved
Relocate Section:					
0	0	SMF80DTP	1	Binary	Data type
1	1	SMF80DLN	1	Binary	Length of data that follows
2	2	SMF80DTA	1-255	mixed	Data
Extended-length Relocate Section:					
0	0	SMF80TP2	2	Binary	Data type
2	2	SMF80DL2	2	Binary	Length of data that follows
4	4	SMF80DA2	variable	EBCDIC	Data

Note 1 — SMF80ATH:

These flags indicate the authority checks made for the user who requested the action. The RACF commands use bits 0, 1, and 3; the RACF requests use bits 0, 2, and 4-7.

- Bit 0 indicates that the user's authority to issue the command or SVC was determined by the checks for a user with the SPECIAL, OPERATIONS, or AUDITOR attribute. This bit indicates that the tests were made, not that the user passed the tests and has authority to issue the command. This bit is not set on if the user has the AUDITOR attribute and entered the command with only those operands that require the AUDITOR attribute.
- Bit 1 indicates that the user has the SPECIAL attribute and used this authority to issue the command. If the user also has the AUDITOR attribute and entered the command with only those operands that require the AUDITOR attribute, this bit is not set on because the user did not use his authority as a user with the SPECIAL attribute.
- Bit 2 is set by RACROUTE REQUEST=AUTH and RACROUTE REQUEST=DEFINE and indicates that the user has the OPERATIONS attribute and used this authority to obtain access to the resource.
- Bit 3 indicates that the user has the AUDITOR attribute and used this authority to issue the command with operands that require the AUDITOR attribute.
- Bit 4 indicates that the user has authority because the exit routine indicated that the request is to be accepted without any further authority checks.
- Bit 5 indicates that resource access was granted by the operator during failsoft processing.
- Bit 6 indicates that *BYPASS* was specified on the user ID field. Access was granted because RACF authority checking was bypassed.
- Bit 7 indicates that the user has the trusted attribute.

Note 2 — SMF80REA:

These flags indicate the reason RACF produced the SMF record.

- Bit 0 is set when there are changes made to a profile in a class specified in the AUDIT operand of the SETROPTS command.
- Bit 1 is set when a user with the AUDITOR attribute specifies the UAUDIT operand on the ALTUSER command for a user and the user has changed RACF profiles with a RACF command, or a RACROUTE REQUEST=AUTH or RACROUTE REQUEST=DEFINE has been issued for the user.
- Bit 2 is set when a user with the AUDITOR attribute specifies the SAUDIT operand on the SETROPTS command and a user with the SPECIAL attribute has changed RACF profiles with a RACF command. However, if a user has both the SPECIAL and AUDITOR attributes and issues a command with operands that require only the AUDITOR attribute, RACF does not log this activity because SPECIAL authority was not used.
- Bit 3 is set if:
 - The AUDIT option in the resource profile specifies that attempts to access the resource be logged.
 - The RACROUTE REQUEST=AUTH exit routine specifies unconditional logging.
 - The console operator grants the resource access during failsoft processing.
- Bit 4 is set when the RACROUTE REQUEST=VERIFY fails to verify a user because of an invalid group, password, terminal, or OIACARD, or initACEE fails because a certificate is not defined or is not trusted.
- Bit 5 is set if the RVARY or SETROPTS command produced the SMF record. (The execution of these two commands always produce an SMF record.)

SMF Records–Type 80

- Bit 6 is set when a user with the AUDITOR attribute specifies logging of command violations (with the CMDVIOL operand on the SETROPTS command) and RACF detects a violation.
- Bit 7 is set when attempts to access a RACF-protected resource are being logged, as requested by the GLOBALAUDIT option in the resource profile.

Note 3 — SMF80ERR:

These flags indicate errors during command processing and the extent of the processing.

- Bit 0 indicates that an error occurred that prevented the command from completing all updates requested, and the command was unable to back out the updates already done. If this bit is on, there may be an inconsistency between the profiles on the RACF database, or between the profile for a data set and the RACF-indicator for the data set in the DSCB or catalog. The latter is also indicated by a bit in the command-related information for the ADDSD, ALTDSD, and DELDSD commands. For some commands (for example, ADDUSER), the inconsistency means an incompletely defined resource. For other commands, where the profiles are already defined (for example, ALTUSER), the inconsistency means that all changes were not made, but the profiles are still usable.

This bit indicates a terminating error and should not be confused with a keyword violation or processing error where the command continues processing other operands.

- Bit 1 indicates that none of the requested changes were made, because either (1) a terminating error occurred before the changes were made, or (2) the command was able to back out the changes after a terminating error.

Table of Event Codes and Event Code Qualifiers

This table describes the SMF80EVT (event code) and SMF80EVQ (event code qualifier) fields.

The event code qualifier is 0 if the recorded event is not a violation or a warning. There are exceptions for event code 1 (Job initiation/TSO logon/logoff); event qualifier codes 8, 12, 13 and 32 are not violations or warnings.

For event codes 8 through 25, an event code qualifier of 1 indicates one of the following:

- The command user is not RACF-defined.
- The command user is not authorized to change the requested profiles on the RACF database.
- The command user does not have sufficient authority for any of the operands on the command.

For event codes 8 through 25, an event code qualifier of 2 indicates that the command user does not have sufficient authority to specify some of the operands, but RACF performed the processing for the operands for which the user has sufficient authority.

Event code qualifiers of 3 and 4 apply to the ADDSD, ALTDSD, and DELDSD commands. They indicate whether the retrieval of the data set affected by the SECLABEL change was successful (3) or not (4).

For detailed descriptions of the SMF event code qualifiers, refer to Appendix E, “Event Code Qualifier Descriptions” on page 421.

Event 1(1): JOB INITIATION / TSO LOGON/LOGOFF (detected by RACINIT request)

Code Qualifier Dec(Hex)	Description	Relocate type sections (Possible SMF80DTP/SMF80DA2 Values)
0(0)	Successful Initiation	1, 17, 20, 46, 47, 49, 53, 55, 331, 332
1(1)	Password not valid	
2(2)	Group not valid	
3(3)	OIDCARD not valid	
4(4)	Terminal/console not valid	
5(5)	Application not valid	
6(6)	Revoked user attempting access	
7(7)	User ID automatically revoked	
8(8)	Successful termination	
9(9)	Undefined user ID	
10(A)	Insufficient security label authority	
11(B)	Not authorized to security label	
12(C)	Successful RACINIT initiation	
13(D)	Successful RACINIT delete	
14(E)	System now requires more authority	
15(F)	Remote job entry - job not authorized	
16(10)	SURROGAT class is inactive	
17(11)	Submitter is not authorized by user	
18(12)	Submitter not authorized to security label	
19(13)	User is not authorized to job	
20(14)	WARNING - Insufficient security label authority	
21(15)	WARNING - security label missing from user, job or profile	
22(16)	WARNING - not authorized to security label	
23(17)	Security labels not compatible	
24(18)	WARNING - security labels not compatible	
25(19)	Current PASSWORD has expired	
26(1A)	Invalid new PASSWORD	
27(1B)	Verification failed by installation	
28(1C)	Group access has been revoked	
29(1D)	OIDCARD is required	
30(1E)	Network job entry - job not authorized	
31(1F)	Warning - unknown user from trusted node propagated	
32(20)	Successful initiation using PassTicket	
33(21)	Attempted replay of PassTicket	

SMF Records–Type 80

Event 2(2): RESOURCE ACCESS (detected by RACROUTE REQUEST=AUTH, RACROUTE REQUEST=FASTAUTH and DIRAUTH function)

Code Qualifier Dec(Hex)	Description	Relocate type sections (Possible SMF80DTP/SMF80DA2 Values)
0(0)	Successful access	1, 3, 4, 5, 15, 16, 17, 20, 33, 38, 46, 48, 49, 51, 53, 54, 55, 64, 65, 66, 331, 332 (see Notes 1 and 2)
1(1)	Insufficient authority	
2(2)	Profile not found - RACFIND specified on macro	
3(3)	Access permitted due to warning	
4(4)	Failed due to PROTECTALL	
5(5)	WARNING issued due to PROTECTALL	
6(6)	Insufficient CATEGORY/SECLEVEL	
7(7)	Insufficient security label authority	
8(8)	WARNING - security label missing from job, user, or profile	
9(9)	WARNING - insufficient security label authority	
10(A)	WARNING - Data set not cataloged	
11(B)	Data set not cataloged	
12(C)	Profile not found - required for authority checking	
13(D)	WARNING - insufficient CATEGORY/SECLEVEL	
14(E)	WARNING - Non-MAIN execution environment detected while in ENHANCED PGMSECURITY mode. Conditional access or use of EXECUTE-controlled program temporarily allowed.	
15(F)	Conditional access or use of EXECUTE-controlled program allowed through BASIC mode program while in ENHANCED PGMSECURITY mode.	

Note 1: The SMF80DTP value 4 (access authority allowed) can be less than the SMF80DTP value 3 (access authority requested) in two cases:

- When RACF authorizes access to a user who requested access to a database because the user has the OPERATIONS attribute.
- When the RACROUTE REQUEST=AUTH exit routine returns a return code of 12, which indicates that the request should be granted.

Note 2: The SMF80DTP value of 16 appears only when the RACROUTE REQUEST=AUTH received an old volume (OLDVOL) as input. The value of 33 appears when a generic profile is used.

Event 3(3): ADDVOL/CHGVOL (detected by RACROUTE REQUEST=DEFINE TYPE=ADDVOL or CHGVOL)

Code Qualifier Dec(Hex)	Description	Relocate type sections (Possible SMF80DTP/SMF80DA2 Values)
0(0)	Successful processing of new volume	1, 4, 5, 15, 16, 17, 33, 38, 44, 46, 49, 53, 55, 331, 332 (see Note)
1(1)	Insufficient authority (DATASET only)	
2(2)	Insufficient security label authority	

Event 3(3): ADDVOL/CHGVOL (detected by RACROUTE REQUEST=DEFINE TYPE=ADDVOL or CHGVOL)

Code Qualifier Dec(Hex)	Description	Relocate type sections (Possible SMF80DTP/SMF80DA2 Values)
3(3)	Less specific profile exists with different seclabel	

Note: The SMF80DTP value of 16 appears only when the RACROUTE REQUEST=AUTH received an old volume (OLDVOL) as input. The value of 33 appears when a generic profile is used.

Event 4(4): RENAME RESOURCE (detected by RACROUTE REQUEST=DEFINE with TYPE=DEFINE and NEWNAME specified)

Code Qualifier Dec(Hex)	Description	Relocate type sections (Possible SMF80DTP/SMF80DA2 Values)
0(0)	Successful rename	1, 2, 5, 15, 17, 33, 38, 44, 46, 49, 53, 55, 331, 332
1(1)	Group not valid	
2(2)	User not in group	
3(3)	Insufficient authority	
4(4)	Resource name already defined	
5(5)	User not defined to RACF	
6(6)	Resource not protected	
7(7)	WARNING - resource not protected	
8(8)	User in second qualifier is not RACF-defined	
9(9)	Less specific profile exists with different SECLABEL	
10(A)	Insufficient security label authority	
11(B)	Resource not protected by security label	
12(C)	New name not protected by security label	
13(D)	New SECLABEL must dominate old SECLABEL	
14(E)	Insufficient security label authority	
15(F)	WARNING - resource not protected by security label	
16(10)	WARNING - new name not protected by security label	
17(11)	WARNING - new SECLABEL must dominate old SECLABEL	

Note: In cases where the RACROUTE REQUEST=DEFINE is used to rename a resource (SMF80EVT=4), the data type 33 relocate section can hold a resource name that is either the old name or the new name, or it can hold the generic profile that protects the old or the new name.

Event 5(5): DELETE RESOURCE (detected by RACROUTE REQUEST=DEFINE, TYPE=DELETE or DELETE)

Code Qualifier Dec(Hex)	Description	Relocate type sections (Possible SMF80DTP/SMF80DA2 Values)
0(0)	Successful scratch	1, 5, 15, 17, 33, 38, 44, 46, 49, 53, 55, 331, 332
1(1)	Resource not found	
2(2)	Invalid volume identification (DATASET only)	

SMF Records–Type 80

Event 6(6): DELETE 1 VOLUME OF MULTIVOLUME RESOURCE (detected by RACROUTE REQUEST=DEFINE, TYPE=DELETE)

Code Qualifier Dec(Hex)	Description	Relocate type sections (Possible SMF80DTP/SMF80DA2 Values)
0(0)	Successful deletion	1, 5, 8, 15, 17, 38, 44, 46, 49, 53, 55, 331, 332

Event 7(7): DEFINE RESOURCE (detected by RACROUTE REQUEST=DEFINE, TYPE=DEFINE)

Code Qualifier Dec(Hex)	Description	Relocate type sections (Possible SMF80DTP/SMF80DA2 Values)
0(0)	Successful definition	1, 5, 15, 17, 18, 19, 33, 38, 44, 46, 49, 53, 55, 331, 332
1(1)	Group undefined	
2(2)	User not in group	
3(3)	Insufficient authority	
4(4)	Resource name already defined	
5(5)	User not defined to RACF	
6(6)	Resource not protected	
7(7)	WARNING - resource not protected	
8(8)	WARNING - security label missing from job, user, or profile	
9(9)	WARNING - insufficient security label authority	
10(A)	User in second qualifier is not RACF-defined	
11(B)	Insufficient security label authority	
12(C)	Less specific profile exists with a different SECLABEL	

EVENT Dec(Hex)	Command	Code Qualifier Dec(Hex)	Description	Relocate type sections (Possible SMF80DTP/SMF80DA2 Values)
8(8)	ADDSD	0(0)	No violations detected	6, 7, 10, 13, 33, 38, 40, 44, 49, 50, 51, 53, 55, 62, 63, 331, 332
		1(1)	Insufficient authority (no update to RACF database)	
		2(2)	Keyword violations detected (partial update to RACF database)	
		3(3)	Successful retrieval of data set names affected by a SECLABEL change	
9(9)	ADDGROUP	0(0)	No violations detected	6, 7, 37, 38, 44, 49, 53, 55, 63, 301, 331, 332
		1(1)	Insufficient authority (no update to RACF database)	
		2(2)	Keyword violations detected (partial update to RACF database)	

SMF Records–Type 80

EVENT Dec(Hex)	Command	Code Qualifier Dec(Hex)	Description	Relocate type sections (Possible SMF80DTP/SMF80DA2 Values)
10(A)	ADDUSER	0(0)	No violations detected	6, 7, 8, 28, 37, 38, 40, 44, 49, 53, 55, 301, 331, 332
		1(1)	Insufficient authority (no update to RACF database)	
		2(2)	Keyword violations detected (partial update to RACF database)	
11(B)	ALTDSD	0(0)	No violations detected	6, 7, 10, 11, 33, 38, 40, 41, 44, 49, 50, 51, 53, 55, 62, 63, 331, 332
		1(1)	Insufficient authority (no update to RACF database)	
		2(2)	Keyword violations detected (partial update to RACF database)	
		3(3)	Successful retrieval of data set names affected by a SECLABEL change	
12(C)	ALTGROUP	0(0)	No violations detected	6, 7, 37, 38, 44, 49, 53, 55, 301, 331, 332
		1(1)	Insufficient authority (no update to RACF database)	
		2(2)	Keyword violations detected (partial update to RACF database)	
13(D)	ALTUSER	0(0)	No violations detected	6, 7, 8, 28, 37, 38, 40, 41, 44, 49, 53, 55, 301, 331, 332
		1(1)	Insufficient authority (no update to RACF database)	
		2(2)	Keyword violations detected (partial update to RACF database)	
14(E)	CONNECT	0(0)	No violations detected	6, 38, 49, 53, 55, 331, 332
		1(1)	Insufficient authority (no update to RACF)	
		2(2)	Keyword violations detected (partial update to RACF database)	
15(F)	DELDSD	0(0)	No violations detected	6, 38, 49, 50, 51, 53, 55, 62, 63, 331, 332
		1(1)	Insufficient authority (no update to RACF database)	
		2(2)	Keyword violations detected (partial update to RACF database)	
		3(3)	Successful retrieval of data set names affected by a SECLABEL change	
		4(4)	Error during retrieval of data set names affected by a SECLABEL change	

SMF Records–Type 80

EVENT Dec(Hex)	Command	Code Qualifier Dec(Hex)	Description	Relocate type sections (Possible SMF80DTP/SMF80DA2 Values)
16(10)	DELGROUP	0(0)	No violations detected	6, 38, 44, 49, 53, 55, 331, 332
		1(1)	Insufficient authority (no update to RACF database)	
		2(2)	Keyword violations detected (partial update to RACF database)	
17(11)	DELUSER	3(0)	No violations detected	6, 38, 44, 49, 53, 55, 331, 332
		1(1)	Insufficient authority (no update to RACF database)	
		2(2)	Keyword violations detected (partial update to RACF database)	
18(12)	PASSWORD	0(0)	No violations detected	6, 38, 49, 53, 331, 332
		1(1)	Insufficient authority (no update to RACF database)	
		2(2)	Keyword violations detected (partial update to the RACF database)	
19(13)	PERMIT	0(0)	No violation detected	6, 9, 12, 13, 14, 17, 26, 38, 39, 49, 53, 55, 331, 332
		1(1)	Insufficient authority (no update to RACF database)	
		2(2)	Insufficient authority (partial update to RACF database)	
20(14)	RALTER	0(0)	No violations detected	6, 7, 9, 10, 11, 17, 24, 25, 29, 33, 38, 40, 41, 44, 49, 50, 51, 53, 55, 331, 332
		1(1)	Insufficient authority (no update to RACF database)	
		2(2)	Keyword violations detected (partial update to RACF database)	
21(15)	RDEFINE	0(0)	No violations detected	6, 7, 9, 13, 17, 24, 29, 33, 38, 40, 44, 49, 50, 51, 53, 55, 331, 332
		1(1)	Insufficient authority (no update to RACF database)	
		2(2)	Keyword violations detected (partial update to RACF database)	
22(16)	RDELETE	0(0)	No violations detected	6, 9, 17, 38, 44, 49, 50, 51, 53, 55, 331, 332
		1(1)	Insufficient authority (no update to RACF database)	
		2(2)	Keyword violations detected (partial update to RACF database)	
23(17)	REMOVE	0(0)	No violations detected	6, 17, 38, 49, 53, 55, 331, 332
		1(1)	Insufficient authority (no update to RACF database)	
		2(2)	Keyword violations detected (partial update to RACF database)	

SMF Records–Type 80

EVENT Dec(Hex)	Command	Code Qualifier Dec(Hex)	Description	Relocate type sections (Possible SMF80DTP/SMF80DA2 Values)
24(18)	SETROPTS	0(0)	No violations detected	6, 21, 22, 23, 27, 32, 34, 35, 36, 42, 43, 44, 45, 49, 53, 55, 331, 332
		1(1)	Insufficient authority (no update to RACF database)	
		2(2)	Keyword violations detected (partial update to RACF database)	
25(19)	RVARY	0(0)	No violations detected	6, 27, 30, 31, 49, 53, 55, 331, 332
		1(1)	Insufficient authority (no update to RACF database)	
		2(2)	Keyword violations detected (partial update to RACF database)	
26(1A)	APPC SESSION ESTABLISHMENT	0(0)	Partner verification was successful	1, 17, 33, 38, 49, 53, 55, 331, 332
		1(1)	Session established without verification	
		2(2)	Local LU key will expire in <= 5 days	
		3(3)	Partner LU access has been revoked	
		4(4)	Partner LU key does not match this LU key	
		5(5)	Session terminated for security reason	
		6(6)	Required SESSION KEY not defined	
		7(7)	Possible security attack by partner LU	
		8(8)	SESSION KEY not defined for partner LU	
		9(9)	SESSION KEY not defined for this LU	
		10(A)	SNA security-related protocol error	
		11(B)	Profile change during verification	
12(C)	Expired SESSION KEY			
27(1B)	GENERAL	0(0)	General purpose auditing	17, 46, 49, 53, 55, 331, 332
28(1C)	DIRECTORY SEARCH	0(0)	Access allowed	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 291, 295, 297, 298, 299, 307, 308, 309, 310, 315, 316, 317, 331, 332
		1(1)	Not authorized to search directory	
29(1D)	CHECK ACCESS TO DIRECTORY	0(0)	Access allowed	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264 265, 266, 267, 268, 269, 270, 297, 298, 299, 307, 308, 309, 310, 315, 316, 317, 331, 332
		1(1)	Caller does not have requested access authority	

SMF Records–Type 80

EVENT Dec(Hex)	Command	Code Qualifier Dec(Hex)	Description	Relocate type sections (Possible SMF80DTP/SMF80DA2 Values)
30(1E)	CHECK ACCESS TO FILE	0(0)	Access allowed	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264,
		1(1)	Caller does not have requested access authority	265, 266, 267, 268, 269, 270, 298, 299, 307, 308, 309, 310, 315, 316, 317, 331, 332
31(1F)	CHAUDIT	0(0)	File's audit options changed	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264,
		1(1)	Caller does not have authority to change user audit options of specified file	265, 266, 292, 293, 294, 307, 308, 309, 310, 315, 316, 317, 331, 332
		2(2)	Caller does not have authority to change auditor audit options	
32(20)	CHDIR	0(0)	Current working directory changed	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264,
		*	Failures logged as directory search event types	265, 266, 315, 316, 317, 331, 332
33(21)	CHMOD	0(0)	File's mode changed	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 263, 264, 265,
		1(1)	Caller does not have authority to change mode of specified file	266, 289, 290, 296, 307, 308, 309, 310, 315, 316, 317, 331, 332
34(22)	CHOWN	0(0)	File's owner or group owner changed	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264,
		1(1)	Caller does not have authority to change owner or group owner of specified file	265, 266, 280, 281, 307, 308, 309, 310, 315, 316, 317, 331, 332
35(23)	CLEAR SETID BITS FOR FILE	0(0)	S_ISUID, S_ISGID, and S_ISVTX bits changed to zero (write) No failure cases	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 289, 290, 317, 331, 332
36(24)	EXEC WITH SETUID/SETGID	0(0)	Successful change of z/OS UNIX user identifiers (UIDs) and z/OS UNIX group identifiers (GIDs). No failure cases. Access to program file is audited via an internal open	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 272, 273, 274, 275, 276, 277, 317, 331, 332
37(25)	GETPSENT	0(0)	Access allowed	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 282, 283, 284,
		1(1)	Not authorized to access specified process	288, 317, 331, 332
38(26)	INITIALIZE z/OS UNIX PROCESS (DUB)	0(0)	z/OS UNIX process successfully initiated	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 317, 331, 332
		1(1)	User not defined as a z/OS UNIX user (no user profile or no OMVS segment)	
		2(2)	User incompletely defined as a z/OS UNIX user (no z/OS UNIX user identifier (UID) in user profile)	
		3(3)	User's current group has no z/OS UNIX group identifier (GID).	
39(27)	z/OS UNIX PROCESS COMPLETION (UNDUB)	0(0)	Process completed No failure cases	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 317, 331, 332

SMF Records–Type 80

EVENT Dec(Hex)	Command	Code Qualifier Dec(Hex)	Description	Relocate type sections (Possible SMF80DTP/SMF80DA2 Values)
40(28)	KILL	0(0)	Access allowed	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 282, 283, 284, 288, 300, 317, 331, 332
		1(1)	Not authorized to access specified process	
41(29)	LINK	0(0)	New link created	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 270, 299, 307, 308, 309, 310, 315, 316, 317, 331, 332
		*	Failures logged as directory search or check access event types	
42(2A)	MKDIR	0(0)	Directory successfully created	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 289, 290, 294, 296, 307, 308, 309, 310, 317, 331, 332
		*	Failures logged as directory search or check access event types	
43(2B)	MKNOD	0(0)	Node successfully created	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 289, 290, 294, 296, 307, 308, 309, 310, 317, 331, 332
		*	Failures logged as directory search or check access event types	
44(2C)	MOUNT FILE SYSTEM	0(0)	Successful mount	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 295, 315, 316, 317, 331, 332
		*	Failures logged as ck_priv event type	
45(2D)	OPEN (NEW FILE)	0(0)	File successfully created	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 289, 290, 294, 296, 307, 308, 309, 310, 317, 331, 332
		*	Failures logged as directory search or check access event types	
46(2E)	PTRACE	0(0)	Access allowed	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 282, 283, 284, 285, 286, 287, 288, 317, 331, 332
		1(1)	Not authorized to access specified process	
47(2F)	RENAME	0(0)	Rename successful	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 270, 271, 278, 279, 294, 299, 302, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 331, 332
		*	Failures logged as directory search or check access event types	
48(30)	RMDIR	0(0)	Successful rmdir	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 307, 308, 309, 310, 315, 316, 317, 331, 332
		*	Failures logged as directory search or check access event types	
49(31)	SETEGID	0(0)	Successful change of effective z/OS UNIX group identifier (GID).	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 275, 276, 277, 281, 317, 331, 332
		1(1)	Not authorized to setegid	
50(32)	SETEUID	0(0)	Successful change of effective z/OS UNIX user identifier (UID).	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 272, 273, 274, 280, 317, 331, 332
		1(1)	Not authorized to seteuid	
51(33)	SETGID	0(0)	Successful change of z/OS UNIX group identifiers (GIDs).	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 275, 276, 277, 281, 317, 331, 332
		1(1)	Not authorized to setgid	
52(34)	SETUID	0(0)	Successful change of z/OS UNIX user identifiers (UIDs).	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 272, 273, 274, 280, 317, 331, 332
		1(1)	Not authorized to setuid	

SMF Records–Type 80

EVENT Dec(Hex)	Command	Code Qualifier Dec(Hex)	Description	Relocate type sections (Possible SMF80DTP/SMF80DA2 Values)
53(35)	SYMLINK	0(0)	Successful symlink	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 297, 307, 308, 309, 310, 317, 331, 332
		*	Failures logged as directory search or check access event types	
54(36)	UNLINK	0(0)	Successful unlink	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 302, 307, 308, 309, 310, 315, 316, 317, 331, 332
		*	Failures logged as directory search or check access event types	
55(37)	UNMOUNT THE SYSTEM	0(0)	Successful unmount	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 295, 315, 316, 317, 331, 332
		*	Failures logged as ck_priv event type	
56(38)	CHECK FILE OWNER	0(0)	User is the owner	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 307, 308, 309, 310, 315, 316, 317, 331, 332
		1(1)	User is not the owner	
57(39)	CK_PRIV	0(0)	User is authorized	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 315, 316, 317, 331, 332
		1(1)	User is not authorized to use requested function	
58(3A)	OPEN SLAVE TTY	0(0)	Access allowed	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 282, 283, 284, 288, 317, 331, 332
		1(1)	Not authorized to access specified process	
59(3B)	RACLINK	0(0)	Access allowed	6, 49, 53, 331, 332
		1(1)	Insufficient authority	
		2(2)	Keyword violation detected	
		3(3)	Association already defined	
		4(4)	Association already approved	
		5(5)	Association does not match	
		6(6)	Association does not exist	
		7(7)	Password not valid or user ID is revoked	
60(3C)	CHECK IPC ACCESS	0(0)	Access allowed	17, 49, 56, 256, 257, 258, 259, 260, 261, 262, 265, 266, 267, 268, 269, 303, 304, 305, 306, 317, 331, 332
		1(1)	Caller does not have proper access authority	
61(3D)	MAKE ISP	0(0)	Successful creation of ISP	17, 49, 56, 256, 257, 258, 259, 260, 261, 262, 265, 266, 269, 303, 304, 305, 306, 317, 331, 332
			No failure case	
62(3E)	R_IPC control	0(0)	Access allowed	17, 49, 56, 256, 257, 258, 259, 260, 261, 262, 265, 266, 280, 281, 289, 290, 291, 296, 303, 304, 305, 306, 317, 331, 332
		1(1)	Caller does not have proper authority.	
63(3F)	SETGROUP	0(0)	Access allowed	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 315, 316, 317, 331, 332
		1(1)	Not authorized to access specified process.	
64(40)	CHECK OWNER, TWO FILES	0(0)	User is the owner	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 271, 278, 279, 315, 316, 317, 331, 332
		1(1)	User is not the owner	

SMF Records–Type 80

EVENT Dec(Hex)	Command	Code Qualifier Dec(Hex)	Description	Relocate type sections (Possible SMF80DTP/SMF80DA2 Values)
65(41)	R_AUDIT	0(0)	Successful r_audit No failure case	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264, 317, 331, 332
66(42)	RACDCERT	0(0)	No violation detected	6, 49, 53, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 336, 337, 338, 339
		1(1)	Insufficient authority (no update to RACF database)	
67(43)	INITACEE	0(0)	Successful certificate registration	49, 53, 318, 319, 331, 332
		1(1)	Successful certificate deregistration	
		2(2)	Not authorized to register the certificate	
		3(3)	Not authorized to deregister the certificate	
		4(4)	No user ID found for the certificate	
		5(5)	The certificate is not trusted	
		6(6)	Successful CERTAUTH certificate registration	
		7(7)	Insufficient authority to register the CERTAUTH certificate	
68(44)	GRANT OF INITIAL KERBEROS TICKET (reserved for use by Network Authentication Service)	0(0)	Success	333, 334, 335
		1(1)	Failure	
69(45)	R_PKIServ GENCERT	0(0)	Successful GENCERT request	46, 49, 53, 318, 319, 331, 332, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 357, 358, 359, 373
		1(1)	Insufficient authority for GENCERT	
		2(2)	Successful REQCERT request	
		3(3)	Insufficient authority for REQCERT	
		4(4)	Successful GENRENEW request	
		5(5)	Insufficient authority for GENRENEW	
		6(6)	Successful REQRENEW request	
		7(7)	Insufficient authority for REQRENEW	
70(46)	R_PKIServ EXPORT	0(0)	Successful EXPORT request	46, 49, 53, 331, 332, 343, 344, 351, 359
		1(1)	Insufficient authority for EXPORT	
		2(2)	Incorrect pass phrase specified for EXPORT	

SMF Records–Type 80

EVENT Dec(Hex)	Command	Code Qualifier Dec(Hex)	Description	Relocate type sections (Possible SMF80DTP/SMF80DA2 Values)
71(47)	POLICY DIRECTOR ACCESS CONTROL DECISION (reserved for use by Policy Director Authorization Services Support)	0(0)	Authorized	352, 353, 354, 355, 356, 372
		1(1)	Not authorized but permitted because of warning mode	
		2(2)	Not authorized because of insufficient traverse authority but permitted because of warning mode	
		3(3)	Not authorized because of time-of-day check but permitted because of warning mode	
		4(4)	Not authorized	
		5(5)	Not authorized because of insufficient traverse authority	
		6(6)	Not authorized because of time-of-day check	
72(48)	R_PKIServ QUERY, DETAILS, or VERIFY	0(0)	Successful admin QUERY or DETAILS request	20, 46, 49, 53, 318, 319, 331, 332, 340, 341, 342, 346, 351, 358, 360, 361, 362, 363, 373
		1(1)	Insufficient authority for admin QUERY or DETAILS	
		2(2)	Successful VERIFY request	
		3(3)	Insufficient authority for VERIFY	
		4(4)	Incorrect VERIFY certificate, no record found for this certificate	
73(49)	R_PKIServ UPDATEREQ	0(0)	Successful admin UPDATEREQ request	46, 49, 53, 331, 332, 340, 341, 342, 346, 347, 348, 349, 350, 351, 357, 364, 365
		1(1)	Insufficient authority for admin UPDATEREQ	
74(4A)	R_PKIServ UPDATECERT or REVOKE	0(0)	Successful admin UPDATECERT request	48, 49, 53, 318, 331, 332, 364, 365, 366
		1(1)	Insufficient authority for admin UPDATECERT	
		2(2)	Successful REVOKE request	
		3(3)	Insufficient authority for REVOKE	
75(4B)	SETFACL	0(0)	ACL entry added, changed, or deleted	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 307, 308, 309, 310, 315, 316, 317, 331, 332, 367, 368, 369, 370, 371
		1(1)	Caller does not have authority to change ACL of specified file	
76(4C)	DELFACL	0(0)	Entire ACL removed	17, 49, 53, 55, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 307, 308, 309, 310, 315, 316, 317, 331, 332, 367
		1(1)	Caller does not have authority to remove ACL of specified file	

Table of Relocate Section Variable Data

This table describes the variable data elements of the relocate section.

Data Type (SMF80DTP) Dec(Hex)	Data Length (SMF80DLN)	Format	Description (SMF80DTA)				
1(1)	1-255	EBCDIC	Resource name or old resource name (RACROUTE REQUEST=AUTH or RACROUTE REQUEST=DEFINE)				
2(2)	1-255	EBCDIC	New data set name (RACROUTE REQUEST=DEFINE)				
3(3)	1	Binary	Access authority requested (RACROUTE REQUEST=DEFINE) (see Note 1)				
4(4)	1	Binary	Access authority allowed (RACROUTE REQUEST=AUTH or RACROUTE REQUEST=DEFINE) (see Note 1)				
5(5)	1	Binary	Data set level number (00-99)				
6(6)	1-255	mixed	RACF command-related data (see Table 4)				
7(7)	1-255	EBCDIC	DATA installation-defined data (ADDUSER, ALTUSER, RALTER, RDEFINE, ADDGROUP, ALTGROUPO, ADDSD, ALTDSD)				
8(8)	1-20	EBCDIC	NAME user-name (ADDUSER, ALTUSER)				
9(9)	1-255	EBCDIC	Resource name (PERMIT, RALTER, RDEFINE, RDELETE)				
10(A)	7	EBCDIC	Volume serial (ALTDSD ADDVOL, RALTER ADDVOL, ADDSD VOLUME). When set on, bit 0 of the first byte indicates that the volume was not processed. Bytes 2-7 contain the volume serial number.				
11(B)	7	EBCDIC	Volume serial (ALTDSD DELVOL, RALTER DELVOL). When set on, bit 0 of the first byte indicates that the volume was not processed. Bytes 2-7 contain the volume serial.				
12(C)	9-243		1 to 27 ID names (PERMIT), each 9 bytes long				
		Binary	Byte 1: Processing flags: <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>ID ignored because of processing error (see Note 2)</td> </tr> <tr> <td>1-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Meaning When Set	0	ID ignored because of processing error (see Note 2)
Bit	Meaning When Set						
0	ID ignored because of processing error (see Note 2)						
1-7	Reserved						
EBCDIC	Bytes 2-9: ID name						
13(D)	1-255	EBCDIC	FROM resource name (PERMIT, ADDSD, RDEFINE)				
14(E)	12	EBCDIC	VOLUME volume serial (6 bytes) followed by FVOLUME volume serial (6 bytes) (PERMIT)				
15(F)	6	EBCDIC	VOLSER volume serial (RACROUTE REQUEST=AUTH or RACROUTE REQUEST=DEFINE)				
			(Note that when RACROUTE REQUEST=AUTH receives a DATASET profile as input, the volume serial logged is the first volume serial contained in the profile's list of volume serials.)				
16(10)	6	EBCDIC	OLDVOL volume serial (RACROUTE REQUEST=AUTH or RACROUTE REQUEST=DEFINE)				
			(Note that when RACROUTE REQUEST=AUTH receives a DATASET profile as input, the volume serial logged is the first volume serial contained in the profile's list of volume serials.)				
17(11)	1-8	EBCDIC	Class name (RACROUTE REQUEST=AUTH or RACROUTE REQUEST=DEFINE, RDEFINE, RALTER, RDELETE, PERMIT, or VMXEVENT auditing). For z/OS UNIX, class controlling auditing for the request.				
18(12)	1-255	EBCDIC	MENTITY model resource name (RACROUTE REQUEST=DEFINE)				
19(13)	6	EBCDIC	Volume serial of model resource (RACROUTE REQUEST=DEFINE)				
20(14)	8	EBCDIC	Application name (RACROUTE REQUEST=AUTH or RACROUTE REQUEST=DEFINE processed)				

SMF Records–Type 80

Data Type (SMF80DTP) Dec(Hex)	Data Length (SMF80DLN)	Format	Description (SMF80DTA)																		
21(15)	10		Current class options (set by SETROPTS or RACF initialization)																		
		binary	Byte 1: <table border="1"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Statistics are in effect</td> </tr> <tr> <td>1</td> <td>Auditing is in effect</td> </tr> <tr> <td>2</td> <td>Protection is in effect</td> </tr> <tr> <td>3</td> <td>Generic profile processing is in effect</td> </tr> <tr> <td>4</td> <td>Generic command processing is in effect</td> </tr> <tr> <td>5</td> <td>Global access checking active</td> </tr> <tr> <td>6</td> <td>RACLIST option in effect</td> </tr> <tr> <td>7</td> <td>GENLIST option in effect</td> </tr> </tbody> </table>	Bit	Meaning When Set	0	Statistics are in effect	1	Auditing is in effect	2	Protection is in effect	3	Generic profile processing is in effect	4	Generic command processing is in effect	5	Global access checking active	6	RACLIST option in effect	7	GENLIST option in effect
Bit	Meaning When Set																				
0	Statistics are in effect																				
1	Auditing is in effect																				
2	Protection is in effect																				
3	Generic profile processing is in effect																				
4	Generic command processing is in effect																				
5	Global access checking active																				
6	RACLIST option in effect																				
7	GENLIST option in effect																				
		EBCDIC	Bytes 2-9: Class name Byte 10: <table border="1"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Reserved</td> </tr> <tr> <td>1</td> <td>ALWAYS</td> </tr> <tr> <td>2</td> <td>NEVER</td> </tr> <tr> <td>3</td> <td>SUCCESSSES</td> </tr> <tr> <td>4</td> <td>FAILURES</td> </tr> <tr> <td>5</td> <td>DEFAULT</td> </tr> <tr> <td>6-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Meaning When Set	0	Reserved	1	ALWAYS	2	NEVER	3	SUCCESSSES	4	FAILURES	5	DEFAULT	6-7	Reserved		
Bit	Meaning When Set																				
0	Reserved																				
1	ALWAYS																				
2	NEVER																				
3	SUCCESSSES																				
4	FAILURES																				
5	DEFAULT																				
6-7	Reserved																				
22(16)	8	EBCDIC	Class name from STATISTICS/NOSTATISTICS keyword (SETROPTS)																		
23(17)	8	EBCDIC	Class name from AUDIT/NOAUDIT keyword (SETROPTS)																		
24(18)	2-247	EBCDIC	Resource name from ADDMEM keyword (RDEFINE, RALTER)																		
			Byte 1: <table border="1"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Resource name not processed</td> </tr> <tr> <td>1</td> <td>Resource name ignored because command user lacked sufficient authority to perform the operation</td> </tr> </tbody> </table> Bytes 2-247: Resource name	Bit	Meaning When Set	0	Resource name not processed	1	Resource name ignored because command user lacked sufficient authority to perform the operation												
Bit	Meaning When Set																				
0	Resource name not processed																				
1	Resource name ignored because command user lacked sufficient authority to perform the operation																				
25(19)	2-247	EBCDIC	Resource name from DELMEM keyword (RALTER). Bit 0 of the first byte, when set on, indicates that the resource name was not processed. Bytes 2-247 contain the resource name.																		
26(1A)	8	EBCDIC	Class name from FCLASS keyword (PERMIT)																		
27(1B)	8	EBCDIC	Class name from CLASSACT/NOCLASSACT keyword (SETROPTS, RVARY)																		
28(1C)	9	mixed	Class name from CLAUTH/NOCLAUTH keyword (ADDUSER, ALTUSER). Bit 1 of the first byte, when set on, indicates that the class was ignored because the command user did not have sufficient authority to perform the operation. Bytes 2-9 contain the class name.																		
29(1D)	1-255	EBCDIC	Application data (RDEFINE, RALTER)																		

Data Type (SMF80DTP) Dec(Hex)	Data Length (SMF80DLN)	Format	Description (SMF80DTA)																												
30(1E)	12-55	mixed	<p>RACF database status (RVARY, RACF initialization)</p> <p>Byte 1:</p> <table border="0"> <tr> <td>Bit</td> <td>Meaning When Set</td> </tr> <tr> <td>0</td> <td>Database is active</td> </tr> <tr> <td>1</td> <td>Database is backup</td> </tr> <tr> <td>2-7</td> <td>Reserved</td> </tr> </table> <p>Bytes 2-4: Unit name</p> <p>Bytes 5-10 Volume</p> <p>Byte 11: Sequence number</p> <p>Byte 12: 1-44 character data set name</p>	Bit	Meaning When Set	0	Database is active	1	Database is backup	2-7	Reserved																				
Bit	Meaning When Set																														
0	Database is active																														
1	Database is backup																														
2-7	Reserved																														
31(1F)	1-44	EBCDIC	Data set name from DATASET operand (RVARY)																												
32(20)	89	mixed	<table border="0"> <tr> <td>Byte</td> <td>Description</td> </tr> <tr> <td>1</td> <td>Password interval value</td> </tr> <tr> <td>2</td> <td>Password history value</td> </tr> <tr> <td>3</td> <td>User ID revoke value</td> </tr> <tr> <td>4</td> <td>Password warning level value</td> </tr> <tr> <td>5-84</td> <td>Password syntax rules value</td> </tr> <tr> <td>85</td> <td>User ID inactive interval</td> </tr> <tr> <td>86-89</td> <td>Indicators</td> </tr> <tr> <td>Bit</td> <td>Meaning When Set</td> </tr> <tr> <td>0</td> <td>MODEL(GDG) in effect</td> </tr> <tr> <td>1</td> <td>MODEL(USER) in effect</td> </tr> <tr> <td>2</td> <td>MODEL(GROUP) in effect</td> </tr> <tr> <td>3</td> <td>GRPLIST in effect</td> </tr> <tr> <td>4-31</td> <td>Reserved</td> </tr> </table>	Byte	Description	1	Password interval value	2	Password history value	3	User ID revoke value	4	Password warning level value	5-84	Password syntax rules value	85	User ID inactive interval	86-89	Indicators	Bit	Meaning When Set	0	MODEL(GDG) in effect	1	MODEL(USER) in effect	2	MODEL(GROUP) in effect	3	GRPLIST in effect	4-31	Reserved
Byte	Description																														
1	Password interval value																														
2	Password history value																														
3	User ID revoke value																														
4	Password warning level value																														
5-84	Password syntax rules value																														
85	User ID inactive interval																														
86-89	Indicators																														
Bit	Meaning When Set																														
0	MODEL(GDG) in effect																														
1	MODEL(USER) in effect																														
2	MODEL(GROUP) in effect																														
3	GRPLIST in effect																														
4-31	Reserved																														
33(21)	2-255	mixed	<p>Byte 1: Processing Flags</p> <table border="0"> <tr> <td>Bit</td> <td>Meaning When Set</td> </tr> <tr> <td>0</td> <td>1=Resource name is generic 0=Generic profile is used</td> </tr> <tr> <td>1</td> <td>1=The old name of a data set renamed by RACROUTE REQUEST=DEFINE. 0=The new name of a data set renamed by RACROUTE REQUEST=DEFINE.</td> </tr> <tr> <td>2-7</td> <td>Reserved</td> </tr> </table> <p>Bytes 2-254: Generic resource name or name of generic profile used</p>	Bit	Meaning When Set	0	1=Resource name is generic 0=Generic profile is used	1	1=The old name of a data set renamed by RACROUTE REQUEST=DEFINE. 0=The new name of a data set renamed by RACROUTE REQUEST=DEFINE.	2-7	Reserved																				
Bit	Meaning When Set																														
0	1=Resource name is generic 0=Generic profile is used																														
1	1=The old name of a data set renamed by RACROUTE REQUEST=DEFINE. 0=The new name of a data set renamed by RACROUTE REQUEST=DEFINE.																														
2-7	Reserved																														
34(22)	8	EBCDIC	Class name from GENERIC/NOGENERIC (SETROPTS)																												
35(23)	8	EBCDIC	Class name from GENCMD/NOGENCMD (SETROPTS)																												
36(24)	8	EBCDIC	Class name from GLOBAL/NOGLOBAL (SETROPTS)																												
37(25)	1-44	EBCDIC	Model name																												
38(26)	8	EBCDIC	User ID or group name that owns the profile (RACROUTE REQUEST=AUTH and RACROUTE REQUEST=DEFINE and all the RACF commands that produce log records, except SETROPTS and RVARY). During DEFINE operations, this field contains the owner that the profile is defined with; in all other operations, it contains the current owner. Thus, for owner changes, it contains the old owner.																												

SMF Records–Type 80

Data Type (SMF80DTP) Dec(Hex)	Data Length (SMF80DLN)	Format	Description (SMF80DTA)																		
39(27)	4-255		Variable number of entity names (PERMIT), each 4 to 42 bytes long																		
		binary	Bytes 1-2: Processing flags: <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Entity ignored because of processing error</td> </tr> <tr> <td>1</td> <td>PROGRAM class entity</td> </tr> <tr> <td>2</td> <td>CONSOLE class entity</td> </tr> <tr> <td>3</td> <td>TERMINAL class entity</td> </tr> <tr> <td>4</td> <td>JESINPUT class entity</td> </tr> <tr> <td>5</td> <td>APPCPORT class entity</td> </tr> <tr> <td>6</td> <td>SYSID entity</td> </tr> <tr> <td>7-15</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Meaning When Set	0	Entity ignored because of processing error	1	PROGRAM class entity	2	CONSOLE class entity	3	TERMINAL class entity	4	JESINPUT class entity	5	APPCPORT class entity	6	SYSID entity	7-15	Reserved
Bit	Meaning When Set																				
0	Entity ignored because of processing error																				
1	PROGRAM class entity																				
2	CONSOLE class entity																				
3	TERMINAL class entity																				
4	JESINPUT class entity																				
5	APPCPORT class entity																				
6	SYSID entity																				
7-15	Reserved																				
			Byte 3: Entity length																		
		EBCDIC	Bytes 4-end: Entity name																		
40(28)	2-45		Category name (ADDSD, ALTDSD, ADDUSER, ALTUSER, RDEFINE, RALTER commands and RACROUTE REQUEST=DEFINE) to be added to the profile, and organized as follows:																		
		binary	Byte 1 (at offset 0): Processing flags: <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Category name ignored because of processing error</td> </tr> <tr> <td>1-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Meaning When Set	0	Category name ignored because of processing error	1-7	Reserved												
Bit	Meaning When Set																				
0	Category name ignored because of processing error																				
1-7	Reserved																				
		EBCDIC	Bytes 2-end (at offset 1): Category name added																		
41(29)	2-45		Category name (ALTDSD, ALTUSER, and RALTER commands) to be deleted from the profile and organized as follows:																		
		binary	Byte 1 (at offset 0): Processing flags: <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Category name ignored because of processing error</td> </tr> <tr> <td>1-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Meaning When Set	0	Category name ignored because of processing error	1-7	Reserved												
Bit	Meaning When Set																				
0	Category name ignored because of processing error																				
1-7	Reserved																				
		EBCDIC	Bytes 2-end (at offset 1): Category name deleted																		
42(2A)	8	EBCDIC	Class name from SETROPTS RACLIST/NORACLIST																		
43(2B)	8	EBCDIC	Class name from SETROPTS GENLIST/NOGENLIST																		
44(2C)	1-255	mixed	Any segment data, except BASE																		
			Byte 1: <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Keyword ignored because of insufficient authority</td> </tr> <tr> <td>1</td> <td>Delete the segment</td> </tr> <tr> <td>2-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Meaning When Set	0	Keyword ignored because of insufficient authority	1	Delete the segment	2-7	Reserved										
Bit	Meaning When Set																				
0	Keyword ignored because of insufficient authority																				
1	Delete the segment																				
2-7	Reserved																				
			Byte 2-9: Name of segment																		
			Byte 10: Length of subkeyword																		
			Variable length The subkeyword specified																		
			Variable length The value associated with the subkeyword (limited to 245 minus length of subkeyword)																		

Data Type (SMF80DTP) Dec(Hex)	Data Length (SMF80DLN)	Format	Description (SMF80DTA)																				
44(2C)	1-255	mixed	Directed command information <table border="0"> <tr> <td>Byte</td> <td>Description</td> </tr> <tr> <td>1</td> <td>Bit string</td> </tr> <tr> <td>2-9</td> <td>Name of segment - CMDSRC</td> </tr> <tr> <td>10</td> <td>Length of subkeyword - 15</td> </tr> <tr> <td>11-25</td> <td>Subkeyword ORIGINATED_FROM</td> </tr> <tr> <td colspan="2">Variable length</td> </tr> <tr> <td colspan="2">Contains one of the following:</td> </tr> <tr> <td colspan="2">• node.userid.DIRECTED_BY_AT</td> </tr> <tr> <td colspan="2">• node.userid.DIRECTED_BY_ONLYAT</td> </tr> <tr> <td colspan="2">• node.userid.DIRECTED_AUTOMATICALLY</td> </tr> </table>	Byte	Description	1	Bit string	2-9	Name of segment - CMDSRC	10	Length of subkeyword - 15	11-25	Subkeyword ORIGINATED_FROM	Variable length		Contains one of the following:		• node.userid.DIRECTED_BY_AT		• node.userid.DIRECTED_BY_ONLYAT		• node.userid.DIRECTED_AUTOMATICALLY	
Byte	Description																						
1	Bit string																						
2-9	Name of segment - CMDSRC																						
10	Length of subkeyword - 15																						
11-25	Subkeyword ORIGINATED_FROM																						
Variable length																							
Contains one of the following:																							
• node.userid.DIRECTED_BY_AT																							
• node.userid.DIRECTED_BY_ONLYAT																							
• node.userid.DIRECTED_AUTOMATICALLY																							
44(2C)	1-255	mixed	Directed application update information <table border="0"> <tr> <td>Byte</td> <td>Description</td> </tr> <tr> <td>1</td> <td>Bit string</td> </tr> <tr> <td>2-9</td> <td>Name of segment - APPLSRC</td> </tr> <tr> <td>10</td> <td>Length of subkeyword - 15</td> </tr> <tr> <td>11-25</td> <td>Subkeyword ORIGINATED_FROM</td> </tr> <tr> <td colspan="2">Variable length</td> </tr> <tr> <td colspan="2">node.userid.DIRECTED_AUTOMATICALLY</td> </tr> </table>	Byte	Description	1	Bit string	2-9	Name of segment - APPLSRC	10	Length of subkeyword - 15	11-25	Subkeyword ORIGINATED_FROM	Variable length		node.userid.DIRECTED_AUTOMATICALLY							
Byte	Description																						
1	Bit string																						
2-9	Name of segment - APPLSRC																						
10	Length of subkeyword - 15																						
11-25	Subkeyword ORIGINATED_FROM																						
Variable length																							
node.userid.DIRECTED_AUTOMATICALLY																							
45(2D)	9		Class and logging options from SETROPTS LOGOPTIONS																				
		EBCDIC	Bytes 1-8: Class name																				
		mixed	Byte 9: <table border="0"> <tr> <td>Bit</td> <td>Meaning When Set</td> </tr> <tr> <td>0</td> <td>ALWAYS</td> </tr> <tr> <td>1</td> <td>NEVER</td> </tr> <tr> <td>2</td> <td>SUCCESSSES</td> </tr> <tr> <td>3</td> <td>FAILURES</td> </tr> <tr> <td>4</td> <td>DEFAULTS</td> </tr> <tr> <td>5-7</td> <td>Reserved</td> </tr> </table>	Bit	Meaning When Set	0	ALWAYS	1	NEVER	2	SUCCESSSES	3	FAILURES	4	DEFAULTS	5-7	Reserved						
Bit	Meaning When Set																						
0	ALWAYS																						
1	NEVER																						
2	SUCCESSSES																						
3	FAILURES																						
4	DEFAULTS																						
5-7	Reserved																						
46(2E)	1-255	EBCDIC	Variable length string of data specified on LOGSTR= keyword on RACROUTE macro																				
47(2F)	8	EBCDIC	JOBNAME that user is not authorized to submit for a JESJOBS job																				
48(30)	8	EBCDIC	User ID to whom data is directed (RECVR= keyword on RACROUTE macro)																				
49(31)	1-20	EBCDIC	User name from ACEE																				
50(32)	8	EBCDIC	SECLABEL name (ADDSD, ALTDSD, ALTUSER, RDEFINE, and RALTER commands) to be added to the profile																				
51(33)	8	EBCDIC	SECLABEL name (RACROUTE REQUEST=AUTH or VMXEVENT auditing) of the resource or SECLABEL name (ALTDSD, ALTUSER, RALTER commands) to be deleted from the profile																				
53(35)	80	mixed	User security token, see "RUTKN" in <i>z/OS Security Server RACF Data Areas</i> .																				
54(36)	80	mixed	Resource security token (RACROUTE REQUEST=AUTH) see "RUTKN" in <i>z/OS Security Server RACF Data Areas</i> .																				
55(37)	8	Binary	Key to link audit records together																				
62(3E)	1-44	EBCDIC	Data set name affected by a SECLABEL change (used by SMF Type 83 Records)																				
63(3F)	4	EBCDIC	Link value to connect data sets affected by a SECLABEL change with the RACF command that caused the change																				
64(40)	4	EBCDIC	Link value to connect client and server audit records. A link value may appear for a client or server without a corresponding link value if: <ul style="list-style-type: none"> the client has failed authorization auditing is not performed for both users 																				

SMF Records–Type 80

Data Type (SMF80DTP) Dec(Hex)	Data Length (SMF80DLN)	Format	Description (SMF80DTA)						
65(41)	1	Binary	Flags that indicate ACEE type: <table border="0"> <tr> <td>Bit</td> <td>Meaning When Set</td> </tr> <tr> <td>0</td> <td>0=Unauthenticated client 1=Authenticated client</td> </tr> <tr> <td>1</td> <td>0=Server 1=Reserved</td> </tr> </table>	Bit	Meaning When Set	0	0=Unauthenticated client 1=Authenticated client	1	0=Server 1=Reserved
Bit	Meaning When Set								
0	0=Unauthenticated client 1=Authenticated client								
1	0=Server 1=Reserved								
66(42)	44	EBCDIC	Partitioned data set name						

Note 1: The access flags are:

Bit	Access Authority
0	ALTER
1	CONTROL
2	UPDATE
3	READ
4	NONE
5	EXECUTE (access authority allowed only)

Note 2: This bit is turned on for each ID in the list (data type 12) and each program entity name in the list (data type 39) that was not processed because of a non-terminating error, such as user IDs (specified on the ID operand of the PERMIT command) that are not defined to RACF. If a terminating error, such as a RACF manager error, occurred while processing an ID or entity, this bit is turned on for all remaining IDs or entities that were not processed.

For the PERMIT DELETE command, when no terminating error has occurred, this bit is turned ON only if no entry in the access list was deleted for the ID or entity.

Table of Extended-Length Relocate Section Variable Data

This table describes the variable data elements of the extended-length relocate section.

Data Type (SMF80TP2) Dec(Hex)	Data Length (SMF80DL2)	Format	Audited by Event Code	Description (SMF80DA2)
256(100)	2	Binary	All	Audit function code, indicating the calling service. Refer to the description of IRRPAFC in <i>z/OS Security Server RACF Data Areas</i> .
257(101)	4	Binary	All	Old real z/OS UNIX user identifier (UID)
258(102)	4	Binary	All	Old effective z/OS UNIX user identifier (UID)
259(103)	4	Binary	All	Old saved z/OS UNIX user identifier (UID)
260(104)	4	Binary	All	Old real z/OS UNIX group identifier (GID)
261(105)	4	Binary	All	Old effective z/OS UNIX group identifier (GID)
262(106)	4	Binary	All	Old saved z/OS UNIX group identifier (GID)
263(107)	1-1023	EBCDIC	28,29,30,31,32, 33,34,35,41,42, 43,44,45,47,48, 53,54,55,56,64	Requested pathname (see also data type 299) Note: For events 47 (rename) and 41 (link), this is the old pathname.
264(108)	16	Binary	28,29,30,31,32, 33,34,35,41,42, 43,44,45,47,48, 53,54,55,56,64	File identifier
265(109)	4	Binary	28,29,30,31,32, 33,34,35,41,42, 43,44,45,47,48, 53,54,55,56,64	File owner z/OS UNIX user identifier (UID)
265(109)	4	Binary	60,61,62	IPC key owner z/OS UNIX user identifier (UID)
266(10A)	4	Binary	28,29,30,31,32, 33,34,35,41,42, 43,44,45,47,48, 53,54,55,56,64	File owner z/OS UNIX group identifier (GID)
266(10A)	4	Binary	60,61,62	IPC key owner z/OS UNIX group identifier (GID)

SMF Records–Type 80

Data Type (SMF80TP2) Dec(Hex)	Data Length (SMF80DL2)	Format	Audited by Event Code	Description (SMF80DA2)
267(10B)	1	Binary	28,29,30	Requested access Value Meaning X'04' Read access X'02' Write access X'01' Execute access X'81' Directory search access X'87' Any access Multiple bits may be set.
267(10B)	1	Binary	60	IPC requested access Value Meaning X'00' No access X'02' Write access X'04' Read access X'06' Read and write access
268(10C)	1	Binary	28, 29, 30, 60	Access type (bits used to make access check) Value Meaning 1 'owner' bits 2 'group' bits 3 'other' bits 4 no bits used 5 UID ACL entry 6 GID ACL entry or entries 7 ACL exists but could not be retrieved 8 A restricted user ID was denied access because it was not the file owner and was not explicitly permitted to the file
269(10D)	1	Binary	28,29,30	Access allowed Value Meaning X'04' Read access X'02' Write access X'01' Execute/search Multiple bits may be set.
269(10D)	1	Binary	60	IPC access allowed Value Meaning X'02' Write access X'04' Read access Multiple bits may be set.
270(10E)	1-1023	EBCDIC	28,29,30,41,47	Second requested pathname (see also data type 299) Note: For events 47 (rename) and 41 (link), this is the new pathname.
271(10F)	16	Binary	47,64	Second file identifier
272(110)	4	Binary	36,50,52	New real z/OS UNIX user identifier (UID)
273(111)	4	Binary	36,50,52	New effective z/OS UNIX user identifier (UID)
274(112)	4	Binary	36,50,52	New saved z/OS UNIX user identifier (UID)
275(113)	4	Binary	36,49,51	New real z/OS UNIX group identifier (GID)
276(114)	4	Binary	36,49,51	New effective z/OS UNIX group identifier (GID)
277(115)	4	Binary	36,49,51	New saved z/OS UNIX group identifier (GID)
278(116)	4	Binary	47	Owner z/OS UNIX user identifier (UID) of deleted file

SMF Records–Type 80

Data Type (SMF80TP2) Dec(Hex)	Data Length (SMF80DL2)	Format	Audited by Event Code	Description (SMF80DA2)
278(116)	4	Binary	64	Second file owner z/OS UNIX user identifier (UID)
279(117)	4	Binary	47	Owner z/OS UNIX group identifier (GID) of deleted file
279(117)	4	Binary	64	Second file owner z/OS UNIX group identifier (GID)
280(118)	4	Binary	34,50,52	z/OS UNIX user identifier (UID) input parameter
280(118)	4	Binary	62	IPC owner z/OS UNIX user identifier (UID) input parameter
281(119)	4	Binary	34,49,51	z/OS UNIX group identifier (GID) input parameter
281(119)	4	Binary	62	IPC owner z/OS UNIX group identifier (GID) input parameter
282(11A)	4	Binary	37,40,46,58	Target real z/OS UNIX user identifier (UID)
283(11B)	4	Binary	37,40,46,58	Target effective z/OS UNIX user identifier (UID)
284(11C)	4	Binary	37,40,46,58	Target saved z/OS UNIX user identifier (UID)
285(11D)	4	Binary	46	Target real z/OS UNIX group identifier (GID)
286(11E)	4	Binary	46	Target effective z/OS UNIX group identifier (GID)
287(11F)	4	Binary	46	Target saved z/OS UNIX group identifier (GID)
288(120)	4	Binary	37,40,46,58	Target PID
289(121)	4	Binary	33,35	Old mode
				Bit Meaning 0-19 Reserved 20 S_ISGID bit 21 S_ISUID bit 22 S_ISVTX bit 23-25 Owner permission bits (read/write/execute) 26-28 Group permission bits (read/write/execute) 29-31 Other permission bits (read/write/execute)
289(121)	4	Binary	62	IPC old mode
				Bit Meaning 0-22 Reserved 23-25 Owner permission bits (RW-) 26-28 Group permission bits (RW-) 29-31 Other permission bits (RW-)
290(122)	4	Binary	33,35,42,43,45	New mode
				Bit Meaning 0-19 Reserved 20 S_ISGID bit 21 S_ISUID bit 22 S_ISVTX bit 23-25 Owner permission bits (read/write/execute) 26-28 Group permission bits (read/write/execute) 29-31 Other permission bits (read/write/execute)

SMF Records–Type 80

Data Type (SMF80TP2) Dec(Hex)	Data Length (SMF80DL2)	Format	Audited by Event Code	Description (SMF80DA2)
290(122)	4	Binary	62	IPC new mode Bit Meaning 0-22 Reserved 23-25 Owner permission bits (RW-) 26-28 Group permission bits (RW-) 29-31 Other permission bits (RW-)
291(123)	2	Binary	28	Service that was being processed. Used when data type 256 indicates the calling service was lookup (pathname resolution).
291(123)	2	Binary	62	Service that was being processed. Used when data type 256 indicates the calling service was to remove an ID, set, or setmqb.
292(124)	4	Binary	31	Requested audit options Byte Meaning 1 Read access audit options 2 Write access audit options 3 Execute/search audit options 4 Reserved In each byte, the following flags are defined: Value Meaning X'00' Don't audit any access attempts X'01' Audit successful accesses X'02' Audit failed access attempts X'03' Audit both successful and failed access attempts
293(125)	8	Binary	31	Old audit options (user and auditor) Byte Meaning 1 User read access audit options 2 User write access audit options 3 User execute/search audit options 4 Reserved 5 Auditor read access audit options 6 Auditor write access audit options 7 Auditor execute/search audit options 8 Reserved In each byte, the following flags are defined: Value Meaning X'00' Don't audit any access attempts X'01' Audit successful accesses X'02' Audit failed access attempts X'03' Audit both successful and failed access attempts

SMF Records–Type 80

Data Type (SMF80TP2) Dec(Hex)	Data Length (SMF80DL2)	Format	Audited by Event Code	Description (SMF80DA2)																												
294(126)	8	Binary	31	<p>New audit options (user and auditor)</p> <table border="1"> <thead> <tr> <th>Byte</th> <th>Meaning</th> </tr> </thead> <tbody> <tr><td>1</td><td>User read access audit options</td></tr> <tr><td>2</td><td>User write access audit options</td></tr> <tr><td>3</td><td>User execute/search audit options</td></tr> <tr><td>4</td><td>Reserved</td></tr> <tr><td>5</td><td>Auditor read access audit options</td></tr> <tr><td>6</td><td>Auditor write access audit options</td></tr> <tr><td>7</td><td>Auditor execute/search audit options</td></tr> <tr><td>8</td><td>Reserved</td></tr> </tbody> </table> <p>In each byte, the following flags are defined:</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Meaning</th> </tr> </thead> <tbody> <tr><td>X'00'</td><td>Don't audit any access attempts</td></tr> <tr><td>X'01'</td><td>Audit successful accesses</td></tr> <tr><td>X'02'</td><td>Audit failed access attempts</td></tr> <tr><td>X'03'</td><td>Audit both successful and failed access attempts</td></tr> </tbody> </table>	Byte	Meaning	1	User read access audit options	2	User write access audit options	3	User execute/search audit options	4	Reserved	5	Auditor read access audit options	6	Auditor write access audit options	7	Auditor execute/search audit options	8	Reserved	Value	Meaning	X'00'	Don't audit any access attempts	X'01'	Audit successful accesses	X'02'	Audit failed access attempts	X'03'	Audit both successful and failed access attempts
Byte	Meaning																															
1	User read access audit options																															
2	User write access audit options																															
3	User execute/search audit options																															
4	Reserved																															
5	Auditor read access audit options																															
6	Auditor write access audit options																															
7	Auditor execute/search audit options																															
8	Reserved																															
Value	Meaning																															
X'00'	Don't audit any access attempts																															
X'01'	Audit successful accesses																															
X'02'	Audit failed access attempts																															
X'03'	Audit both successful and failed access attempts																															
295(127)	1-44	EBCDIC	28,44,55	HFS data set name for mounted file system																												
296(128)	4	Binary	33,42,43,45	<p>Requested file mode</p> <table border="1"> <thead> <tr> <th>Bit</th> <th>Meaning</th> </tr> </thead> <tbody> <tr><td>0-19</td><td>Reserved</td></tr> <tr><td>20</td><td>S_ISGID bit</td></tr> <tr><td>21</td><td>S_ISUID bit</td></tr> <tr><td>22</td><td>S_ISVTX bit</td></tr> <tr><td>23-25</td><td>Owner permission bits (read/write/execute)</td></tr> <tr><td>26-28</td><td>Group permission bits (read/write/execute)</td></tr> <tr><td>29-31</td><td>Other permission bits (read/write/execute)</td></tr> </tbody> </table>	Bit	Meaning	0-19	Reserved	20	S_ISGID bit	21	S_ISUID bit	22	S_ISVTX bit	23-25	Owner permission bits (read/write/execute)	26-28	Group permission bits (read/write/execute)	29-31	Other permission bits (read/write/execute)												
Bit	Meaning																															
0-19	Reserved																															
20	S_ISGID bit																															
21	S_ISUID bit																															
22	S_ISVTX bit																															
23-25	Owner permission bits (read/write/execute)																															
26-28	Group permission bits (read/write/execute)																															
29-31	Other permission bits (read/write/execute)																															
296(128)	4	Binary	61,62	<p>IPC requested ISP mode.</p> <table border="1"> <thead> <tr> <th>Bit</th> <th>Meaning</th> </tr> </thead> <tbody> <tr><td>0-22</td><td>Reserved</td></tr> <tr><td>23-25</td><td>Owner permission bits (RW-)</td></tr> <tr><td>26-28</td><td>Group permission bits (RW-)</td></tr> <tr><td>29-31</td><td>Other permission bits (RW-)</td></tr> </tbody> </table>	Bit	Meaning	0-22	Reserved	23-25	Owner permission bits (RW-)	26-28	Group permission bits (RW-)	29-31	Other permission bits (RW-)																		
Bit	Meaning																															
0-22	Reserved																															
23-25	Owner permission bits (RW-)																															
26-28	Group permission bits (RW-)																															
29-31	Other permission bits (RW-)																															
297(129)	1-1023	EBCDIC	28,29,53	Content of symlink																												
298(12A)	1-256	EBCDIC	28,29,30	File name being checked																												
299(12B)	1	Binary	28,29,30, 41,47	<p>Flag indicating whether the requested pathname is the old (or only) pathname or the new pathname. This field is X'01' except for ck_access events where authority to a new name is being checked. The second pathname contains the new name specified.</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Meaning</th> </tr> </thead> <tbody> <tr><td>X'01'</td><td>Old (or only) pathname</td></tr> <tr><td>X'02'</td><td>New pathname</td></tr> </tbody> </table>	Value	Meaning	X'01'	Old (or only) pathname	X'02'	New pathname																						
Value	Meaning																															
X'01'	Old (or only) pathname																															
X'02'	New pathname																															
300(12C)	4	Binary	40	Kill signal code																												
301(12D)	variable	EBCDIC	9,10,12,13	Command segment data																												
302(12E)	1	Binary	47,54	<p>Last link deleted flag</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Meaning</th> </tr> </thead> <tbody> <tr><td>X'00'</td><td>Last link was not deleted</td></tr> <tr><td>X'01'</td><td>Last link was deleted.</td></tr> </tbody> </table>	Value	Meaning	X'00'	Last link was not deleted	X'01'	Last link was deleted.																						
Value	Meaning																															
X'00'	Last link was not deleted																															
X'01'	Last link was deleted.																															
303(12F)	4	Binary	60,61,62	IPC key																												

SMF Records–Type 80

Data Type (SMF80TP2) Dec(Hex)	Data Length (SMF80DL2)	Format	Audited by Event Code	Description (SMF80DA2)						
304(130)	4	Binary	60,61,62	IPC ID						
305(131)	4	Binary	60,61,62	IPC key creator z/OS UNIX user identifier (UID)						
306(132)	4	Binary	60,61,62	IPC key creator z/OS UNIX group identifier (GID)						
307(133)	8	EBCDIC	28,29,30,31,33, 34,41,42,43,45, 47,48,53,54,56	Filepool name						
308(134)	8	EBCDIC	28,29,30,31,33, 34,41,42,43,45, 47,48,53,54,56	Filespace name						
309(135)	4	Binary	28,29,30,31,33, 34,41,42,43,45, 47,48,53,54,56	Inode (file serial number)						
310(136)	4	Binary	28,29,30,31,33, 34,41,42,43,45, 47,48,53,54,56	SCID (file serial number)						
311(137)	8	EBCDIC	47	Second filepool name						
312(138)	8	EBCDIC	47	Second filespace name						
313(139)	4	Binary	47	Second Inode (file serial number)						
314(13A)	4	Binary	47	Second SCID (file serial number)						
315(13B)	4	EBCDIC	28,29,30,31,32, 33,34,41,44,47, 48,54,55,56,57, 63,64	Link value to connect client and server audit records. A link value may appear for a client or server without a corresponding link value if: <ul style="list-style-type: none"> • the client has failed authorization • auditing is not performed for both users 						
316(13C)	1	Binary	28,29,30,31,32, 33,34,41,44,47,48,54, 55,56,57,63,64	Flags that indicate ACEE type: <table style="margin-left: 20px; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Bit</th> <th style="text-align: left;">Meaning</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>0=Unauthenticated client; 1=Authenticated client</td> </tr> <tr> <td>1</td> <td>0=Server 1=Reserved</td> </tr> </tbody> </table>	Bit	Meaning	0	0=Unauthenticated client; 1=Authenticated client	1	0=Server 1=Reserved
Bit	Meaning									
0	0=Unauthenticated client; 1=Authenticated client									
1	0=Server 1=Reserved									
317(13D)	1	Binary	28,29,30,31,32, 33,34,35,36,37, 38,39,40,41,42, 43,44,45,46,47, 48,49,50,51,52, 53,54,55,56,57, 58,60,61,62,63, 64,65	<table style="margin-left: 20px; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Value X'80'</th> <th style="text-align: left;">Meaning</th> </tr> </thead> <tbody> <tr> <td></td> <td>Indicates a default z/OS UNIX security environment is in effect.</td> </tr> </tbody> </table>	Value X'80'	Meaning		Indicates a default z/OS UNIX security environment is in effect.		
Value X'80'	Meaning									
	Indicates a default z/OS UNIX security environment is in effect.									
318(13E)	variable	EBCDIC	66, 67	Certificate serial number						
319(13F)	variable	EBCDIC	66, 67	Certificate issuer's distinguished name						
320(140)	1-237	Char	66	Ring name						
321(141)	1-64	Char	66	C from SUBJECTSDN						
322(142)	1-64	Char	66	SP from SUBJECTSDN						
323(143)	1-64	Char	66	L from SUBJECTSDN						
324(144)	1-64	Char	66	O from SUBJECTSDN						
325(145)	1-64	Char	66	OU from SUBJECTSDN						
326(146)	1-64	Char	66	T from SUBJECTSDN						
327(147)	1-64	Char	66	CN from SUBJECTSDN						
328(148)	1-255	EBCDIC	66	SDNFILTER filter name						
329(149)	1-255	EBCDIC	66	IDNFILTER filter name						
330(14A)	1-255	EBCDIC	66	CRITERIA or NEWCRITERIA value						
331(14B)	1-255	EBCDIC	ALL events except 68	Subject's distinguished name						
332(14C)	1-255	EBCDIC	ALL events except 68	Issuer's distinguished name						
333(14D)	1-240	EBCDIC	68	Kerberos principal name (reserved for use by Network Authentication Service)						

SMF Records–Type 80

Data Type (SMF80TP2) Dec(Hex)	Data Length (SMF80DL2)	Format	Audited by Event Code	Description (SMF80DA2)										
334(14E)	7-22	EBCDIC	68	Kerberos login request source (reserved for use by Network Authentication Service)										
335(14F)	1-10	EBCDIC	68	Kerberos KDC status code (reserved for use by Network Authentication Service)										
336(150)	1-255	EBCDIC	66	ALTNAME IP Address										
337(151)	1-255	EBCDIC	66	ALTNAME EMail										
338(152)	1-255	EBCDIC	66	ALTNAME Domain										
339(153)	1-255	EBCDIC	66	ALTNAME URI										
340(154)	1	Binary	69	IRRSXP00 flags: <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>"handshake" specified in KeyUsage field</td> </tr> <tr> <td>1</td> <td>"dataencrypt" specified in KeyUsage field</td> </tr> <tr> <td>2</td> <td>"certsign" specified in KeyUsage field</td> </tr> <tr> <td>3</td> <td>"docsign" specified in KeyUsage field</td> </tr> </tbody> </table>	Bit	Meaning	0	"handshake" specified in KeyUsage field	1	"dataencrypt" specified in KeyUsage field	2	"certsign" specified in KeyUsage field	3	"docsign" specified in KeyUsage field
Bit	Meaning													
0	"handshake" specified in KeyUsage field													
1	"dataencrypt" specified in KeyUsage field													
2	"certsign" specified in KeyUsage field													
3	"docsign" specified in KeyUsage field													
341(155)	10	EBCDIC	69	Requested NotBefore field in the format yyyy/mm/dd										
342(156)	10	EBCDIC	69	Requested NotAfter field in the format yyyy/mm/dd										
343(157)	8	EBCDIC	69, 70	IRRSXP00 target user ID										
344(158)	1-32	EBCDIC	69, 70	IRRSXP00 target label										
345(159)	1-45	EBCDIC	69	IRRSXP00 SignWith field										
346(15A)	1-255	EBCDIC	69	Requested Subject's DN										
347(15B)	1-64	EBCDIC	69	Requested AltIPAddr field										
348(15C)	1-255	EBCDIC	69	Requested AltURI field										
349(15D)	1-100	EBCDIC	69	Requested AltEmail field										
350(15E)	1-100	EBCDIC	69	Requested AltDomain field										
351(15F)	1-56	EBCDIC	69, 70	IRRSXP00 CertId										
352(160)	1-4096	EBCDIC	71	Policy Director protected object (reserved for use by Policy Director Authorization Services Support)										
353(161)	1-1024	EBCDIC	71	Requested Policy Director permissions (reserved for use by Policy Director Authorization Services Support)										
354(162)	8	EBCDIC	71	Policy Director principal userID (reserved for use by Policy Director Authorization Services Support)										
355(163)	36	EBCDIC	71	Principal ID string in the format <i>nnnnnnnn-nnnn-nnnn-nnnnnnnnnnnnn</i> where <i>n</i> is any hexadecimal digit (reserved for use by Policy Director Authorization Services Support)										
356(164)	4	Binary	71	Policy Director quality of protection value (reserved for use by Policy Director Authorization Services Support)										
357(165)	1024	EBCDIC	69, 70, 73	HostIDMappings extension data										
358(166)	32	EBCDIC	70	Certificate requestor's name										
359(167)	1	Binary	69, 70	IRRSXP00 flags byte 2 <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Pass phrase specified</td> </tr> </tbody> </table>	Bit	Meaning	0	Pass phrase specified						
Bit	Meaning													
0	Pass phrase specified													

Data Type (SMF80TP2) Dec(Hex)	Data Length (SMF80DL2)	Format	Audited by Event Code	Description (SMF80DA2)								
360(168)	32	EBCDIC	72	Certificate or certificate request status: <ul style="list-style-type: none"> • Pending approval • Approved • Completed • Rejected • Rejected, User Notified • Active • Expired • Revoked • Revoked, Expired 								
361(169)	10	EBCDIC	72	Creation date in the format yyyy/mm/dd								
362(16A)	10	EBCDIC	72	Last modified in the format yyyy/mm/dd								
363(16B)	1–255	EBCDIC	72	Certificate serial number for previously issued certificate								
364(16C)	4	Binary	73, 74	Action taken on certificate or certificate request								
365(16D)	1–64	EBCDIC	74	Action comment								
366(16E)	4	Binary	74	Certificate revocation reason								
367(16F)	1	Binary	75, 76	ACL type <table border="0"> <tr> <td>Value</td> <td>Meaning</td> </tr> <tr> <td>X'80'</td> <td>Access ACL</td> </tr> <tr> <td>X'40'</td> <td>File model</td> </tr> <tr> <td>X'20'</td> <td>Directory model</td> </tr> </table>	Value	Meaning	X'80'	Access ACL	X'40'	File model	X'20'	Directory model
Value	Meaning											
X'80'	Access ACL											
X'40'	File model											
X'20'	Directory model											
368(170)	1	Unsigned	75	Effective ACL entry operation type <table border="0"> <tr> <td>Value</td> <td>Meaning</td> </tr> <tr> <td>1</td> <td>Add</td> </tr> <tr> <td>2</td> <td>Modify</td> </tr> <tr> <td>3</td> <td>Delete</td> </tr> </table>	Value	Meaning	1	Add	2	Modify	3	Delete
Value	Meaning											
1	Add											
2	Modify											
3	Delete											
369(171)	5	Binary	75	ACL entry identifier. This consists of a 1–byte type code followed by the 4–byte hexadecimal UID or GID value. <table border="0"> <tr> <td>Value</td> <td>Meaning</td> </tr> <tr> <td>X'01'</td> <td>User (UID) entry</td> </tr> <tr> <td>X'02'</td> <td>Group (GID) entry</td> </tr> </table>	Value	Meaning	X'01'	User (UID) entry	X'02'	Group (GID) entry		
Value	Meaning											
X'01'	User (UID) entry											
X'02'	Group (GID) entry											
370(172)	1	Binary	75	Old ACL entry bits for modify and delete operations.								
371(173)	1	Binary	75	New ACL entry bits for add and modify operations.								
372(174)	1	Binary	71	Policy Director credential type flag reserved for use by Policy Director Authorization Services Support) <table border="0"> <tr> <td>Value</td> <td>Meaning</td> </tr> <tr> <td>X'00'</td> <td>Unauthenticated</td> </tr> <tr> <td>X'01'</td> <td>Authenticated</td> </tr> </table>	Value	Meaning	X'00'	Unauthenticated	X'01'	Authenticated		
Value	Meaning											
X'00'	Unauthenticated											
X'01'	Authenticated											
373(175)	1–64	EBCDIC	69, 72	E-mail address for notification purposes.								

Table of Data Type 6 Command-Related Data

- ADDGROUP
- ADDSD
- ADDUSER
- ALTDSD
- ALTGROUP
- ALTUSER
- CONNECT

Data Type 6

- DELDSD
- DELGROUP
- DELUSER
- PASSWORD
- PERMIT
- RACDCERT
- RACLINK
- RALTER
- RDEFINE
- RDELETE
- REMOVE
- RVARY
- SETROPTS

This table describes the RACF command-related data associated with data type 6. The actual format and content of the data depends upon the command being logged. Command-related data will not appear in the SMF record if the command user is not RACF-defined. Some of the commands also omit the command-related data if the user is not authorized for the requested profile on the RACF database.

The table is arranged by event code. In each description, the keyword flags contain one flag for each possible keyword that you can specify (explicitly or by default) on the command. The 'flags for keywords specified' field indicates whether the keyword was specified or defaulted.

The 'flags for keywords ignored because of insufficient authority' indicates whether the keyword was ignored because the user did not have sufficient authority to use the keyword. The event code qualifier (SMF80EVQ), described in Table 1, is set to 1 if the command user does not have sufficient authority for any of the keywords specified or taken as defaults. The event code qualifier is set to 2 if the command user does not have sufficient authority for some (but not all) of the keywords specified or taken as defaults. In the latter case, the command continues processing the authorized operands.

The 'flags for keywords ignored due to error conditions' field indicates individual keywords that were not processed for reasons other than insufficient authority. Not all commands (event codes 8-25) have these flags. The keyword errors are not terminating errors (like the errors indicated in SMF80ERR) and the command continues processing other specified operands. In the event of a terminating error, these flags do not necessarily indicate what processing was done or not done. Any keyword errors occurring before the terminating error are indicated, but the keywords not processed because of a terminating error are not indicated. The bits in SMF80ERR indicate whether or not RACF already made changes to the RACF database before the terminating error and if it backed out the changes successfully.

Other fields in the command-related data field indicate the subfields specified (or defaulted) for keywords. The fields are flags for subfields that are keywords (such as SUCCESS subfield of AUDIT); they are data for subfields such as owner name or group name.

For example, if the owner of the profile for USERA issues the command:

```
ALTUSER USERA ADSP GRPACC SPECIAL OWNER(USERB)
```

and USERB, the requested new owner is not RACF-defined, then the command-related data would appear in the log record as:

```
012C0000 00040000 00080000 00E4E2C5  
D9C14040 40000000 00000000 00000000  
00000000 000000E4 E2C5D9C2 40404000  
00000000
```

The first word indicates the keywords specified. The second word indicates the user does not have sufficient authority to use the SPECIAL keyword. The third word indicates there was an error processing the OWNER keyword. At offset X'0D' is the name of the user profile being altered. At offset X'27' is the name of the owner specified on the command. RACF processed the ADSP and GRPACC keywords.

Note: If you use SMF records to reconstruct a RACF database, passwords and OIDCARDS are not contained in the records and require special handling, and statistics updates are not recorded.

Data Type 6

Event Code Dec(Hex)	Command	Data Length	Format	Description																																						
8(8)	ADDSD	2	Binary	Flags for keywords specified: <table border="0"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr> <td colspan="2">Byte 0</td> </tr> <tr> <td>0</td> <td>VOLUME</td> </tr> <tr> <td>1</td> <td>UNIT</td> </tr> <tr> <td>2</td> <td>UACC</td> </tr> <tr> <td>3</td> <td>OWNER</td> </tr> <tr> <td>4</td> <td>AUDIT</td> </tr> <tr> <td>5</td> <td>SET</td> </tr> <tr> <td>6</td> <td>NOSET</td> </tr> <tr> <td>7</td> <td>LEVEL</td> </tr> <tr> <td colspan="2">Byte 1</td> </tr> <tr> <td>0</td> <td>PASSWORD</td> </tr> <tr> <td>1</td> <td>DATA</td> </tr> <tr> <td>2</td> <td>MODEL</td> </tr> <tr> <td>3</td> <td>WARNING</td> </tr> <tr> <td>4</td> <td>GENERIC</td> </tr> <tr> <td>5</td> <td>SECLEVEL</td> </tr> <tr> <td>6</td> <td>ADDCATEGORY</td> </tr> <tr> <td>7</td> <td>NOTIFY</td> </tr> </tbody> </table>	Bit	Keyword Specified	Byte 0		0	VOLUME	1	UNIT	2	UACC	3	OWNER	4	AUDIT	5	SET	6	NOSET	7	LEVEL	Byte 1		0	PASSWORD	1	DATA	2	MODEL	3	WARNING	4	GENERIC	5	SECLEVEL	6	ADDCATEGORY	7	NOTIFY
Bit	Keyword Specified																																									
Byte 0																																										
0	VOLUME																																									
1	UNIT																																									
2	UACC																																									
3	OWNER																																									
4	AUDIT																																									
5	SET																																									
6	NOSET																																									
7	LEVEL																																									
Byte 1																																										
0	PASSWORD																																									
1	DATA																																									
2	MODEL																																									
3	WARNING																																									
4	GENERIC																																									
5	SECLEVEL																																									
6	ADDCATEGORY																																									
7	NOTIFY																																									
		2	Binary	Flags for keywords ignored because of insufficient authority: Same format as flags for keywords specified.																																						
		44	EBCDIC	Data set name																																						
		8	EBCDIC	Type (UNIT keyword)																																						
		1	Binary	Flags for UACC keyword: Note: If this is a non-DFP data set, RACF ignores bit 4 when checking access to data sets. <table border="0"> <thead> <tr> <th>Bit</th> <th>Authority Specified</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>ALTER</td> </tr> <tr> <td>1</td> <td>CONTROL</td> </tr> <tr> <td>2</td> <td>UPDATE</td> </tr> <tr> <td>3</td> <td>READ</td> </tr> <tr> <td>4</td> <td>EXECUTE</td> </tr> <tr> <td>5-6</td> <td>Reserved</td> </tr> <tr> <td>7</td> <td>NONE</td> </tr> </tbody> </table>	Bit	Authority Specified	0	ALTER	1	CONTROL	2	UPDATE	3	READ	4	EXECUTE	5-6	Reserved	7	NONE																						
Bit	Authority Specified																																									
0	ALTER																																									
1	CONTROL																																									
2	UPDATE																																									
3	READ																																									
4	EXECUTE																																									
5-6	Reserved																																									
7	NONE																																									
		8	EBCDIC	User ID or group name (OWNER keyword)																																						
		1	Binary	Flags for AUDIT keyword: (only one set at a time) <table border="0"> <thead> <tr> <th>Bit</th> <th>Option Specified</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>ALL</td> </tr> <tr> <td>1</td> <td>SUCCESS</td> </tr> <tr> <td>2</td> <td>FAILURES</td> </tr> <tr> <td>3</td> <td>NONE</td> </tr> <tr> <td>4-5</td> <td>SUCCESS qualifier codes: '00' — READ '01' — UPDATE '10' — CONTROL '11' — ALTER</td> </tr> <tr> <td>6-7</td> <td>FAILURES qualifier codes: '00' — READ '01' — UPDATE '10' — CONTROL '11' — ALTER</td> </tr> </tbody> </table>	Bit	Option Specified	0	ALL	1	SUCCESS	2	FAILURES	3	NONE	4-5	SUCCESS qualifier codes: '00' — READ '01' — UPDATE '10' — CONTROL '11' — ALTER	6-7	FAILURES qualifier codes: '00' — READ '01' — UPDATE '10' — CONTROL '11' — ALTER																								
Bit	Option Specified																																									
0	ALL																																									
1	SUCCESS																																									
2	FAILURES																																									
3	NONE																																									
4-5	SUCCESS qualifier codes: '00' — READ '01' — UPDATE '10' — CONTROL '11' — ALTER																																									
6-7	FAILURES qualifier codes: '00' — READ '01' — UPDATE '10' — CONTROL '11' — ALTER																																									
		1	Binary	nn (LEVEL keyword)																																						

Event Code Dec(Hex)	Command	Data Length	Format	Description																													
8(8) (Cont.)	ADDSD (Cont.)	1	Binary	Flags for RACF processing:																													
				<table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Data set profile inconsistent with RACF indicator</td> </tr> <tr> <td>1</td> <td>Generic profile name specified</td> </tr> <tr> <td>2</td> <td>FROM entity is longer than 44 characters — entity is passed in relocate type 13</td> </tr> <tr> <td>3–7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Meaning	0	Data set profile inconsistent with RACF indicator	1	Generic profile name specified	2	FROM entity is longer than 44 characters — entity is passed in relocate type 13	3–7	Reserved																			
		Bit	Meaning																														
		0	Data set profile inconsistent with RACF indicator																														
		1	Generic profile name specified																														
		2	FROM entity is longer than 44 characters — entity is passed in relocate type 13																														
		3–7	Reserved																														
		8	EBCDIC	User to be notified when this profile denies access																													
		2	Binary	2	Flags for keywords specified:																												
					<table border="0"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr> <td colspan="2">Byte 0</td> </tr> <tr> <td>0</td> <td>SETONLY</td> </tr> <tr> <td>1</td> <td>TAPE</td> </tr> <tr> <td>2</td> <td>FILESEQ</td> </tr> <tr> <td>3</td> <td>RETPD</td> </tr> <tr> <td>4</td> <td>ERASE</td> </tr> <tr> <td>5</td> <td>FROM</td> </tr> <tr> <td>6</td> <td>FCLASS</td> </tr> <tr> <td>7</td> <td>FVOLUME</td> </tr> <tr> <td colspan="2">Byte 1</td> </tr> <tr> <td>0</td> <td>FGENERIC</td> </tr> <tr> <td>1</td> <td>SECLABEL</td> </tr> <tr> <td>2–7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Keyword Specified	Byte 0		0	SETONLY	1	TAPE	2	FILESEQ	3	RETPD	4	ERASE	5	FROM	6	FCLASS	7	FVOLUME	Byte 1		0	FGENERIC	1	SECLABEL	2–7	Reserved
					Bit	Keyword Specified																											
					Byte 0																												
					0	SETONLY																											
					1	TAPE																											
2	FILESEQ																																
3	RETPD																																
4	ERASE																																
5	FROM																																
6	FCLASS																																
7	FVOLUME																																
Byte 1																																	
0	FGENERIC																																
1	SECLABEL																																
2–7	Reserved																																
Flags for keywords ignored. Same format as flags for keywords specified.																																	
1	EBCDIC	Reserved																															
2	Binary	File sequence number																															
2	Binary	Retention period																															
8	EBCDIC	FROM class name																															
44	EBCDIC	FROM resource name																															
8	EBCDIC	FROM volume serial																															
44	EBCDIC	SECLEVEL name																															
8	EBCDIC	SECLABEL																															
9(9)	ADDGROUP	1	Binary	Flags for keywords specified:																													
				<table border="0"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>SUPGROUP</td> </tr> <tr> <td>1</td> <td>OWNER</td> </tr> <tr> <td>2</td> <td>NOTERMUACC</td> </tr> <tr> <td>3</td> <td>TERMUACC</td> </tr> <tr> <td>4</td> <td>DATA</td> </tr> <tr> <td>5</td> <td>MODEL</td> </tr> <tr> <td>6</td> <td>UNIVERSAL</td> </tr> <tr> <td>7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Keyword Specified	0	SUPGROUP	1	OWNER	2	NOTERMUACC	3	TERMUACC	4	DATA	5	MODEL	6	UNIVERSAL	7	Reserved											
		Bit	Keyword Specified																														
		0	SUPGROUP																														
		1	OWNER																														
		2	NOTERMUACC																														
		3	TERMUACC																														
		4	DATA																														
5	MODEL																																
6	UNIVERSAL																																
7	Reserved																																
1	Binary	Flags for keywords ignored because of insufficient authority: Same format as flags for keywords specified.																															
8	EBCDIC	Group name																															
8	EBCDIC	Superior group name (SUPGROUP keyword)																															
8	EBCDIC	User ID or group name (OWNER keyword)																															

Data Type 6

Event Code Dec(Hex)	Command	Data Length	Format	Description																																																																										
10(A)	ADDUSER	* The data for event code 10 is identical to the data for event code 13, with these exceptions.																																																																												
		4	Binary	Flags for keywords specified:																																																																										
				<table border="1"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr> <td colspan="2">Byte 0</td> </tr> <tr> <td>0</td> <td>DFLTGRP</td> </tr> <tr> <td>*1</td> <td>GROUP</td> </tr> <tr> <td>2</td> <td>PASSWORD</td> </tr> <tr> <td>3</td> <td>NOPASSWORD</td> </tr> <tr> <td>4</td> <td>NAME</td> </tr> <tr> <td>5</td> <td>AUTHORITY</td> </tr> <tr> <td>6</td> <td>DATA</td> </tr> <tr> <td>7</td> <td>GRPACC</td> </tr> <tr> <td colspan="2">Byte 1</td> </tr> <tr> <td>0</td> <td>NOGRPACC</td> </tr> <tr> <td>1</td> <td>UACC</td> </tr> <tr> <td>2</td> <td>ADSP</td> </tr> <tr> <td>3</td> <td>NOADSP</td> </tr> <tr> <td>4</td> <td>OWNER</td> </tr> <tr> <td>5</td> <td>SPECIAL</td> </tr> <tr> <td>6</td> <td>NOSPECIAL</td> </tr> <tr> <td>7</td> <td>OPERATIONS</td> </tr> <tr> <td colspan="2">Byte 2</td> </tr> <tr> <td>0</td> <td>NOOPERATIONS</td> </tr> <tr> <td>1</td> <td>CLAUTH</td> </tr> <tr> <td>2</td> <td>NOCLAUTH</td> </tr> <tr> <td>3</td> <td>AUDITOR</td> </tr> <tr> <td>4</td> <td>NOAUDITOR</td> </tr> <tr> <td>5</td> <td>OIDCARD</td> </tr> <tr> <td>6</td> <td>NOOIDCARD</td> </tr> <tr> <td>*7</td> <td>REVOKE</td> </tr> <tr> <td colspan="2">Byte 3</td> </tr> <tr> <td>*0</td> <td>RESUME</td> </tr> <tr> <td>*1</td> <td>AUDIT</td> </tr> <tr> <td>*2</td> <td>NOAUDIT</td> </tr> <tr> <td>3</td> <td>MODEL</td> </tr> <tr> <td>*4</td> <td>NOMODEL</td> </tr> <tr> <td>5</td> <td>WHEN</td> </tr> <tr> <td>6</td> <td>ADDCATEGORY</td> </tr> <tr> <td>7</td> <td>DELCATEGORY</td> </tr> </tbody> </table>	Bit	Keyword Specified	Byte 0		0	DFLTGRP	*1	GROUP	2	PASSWORD	3	NOPASSWORD	4	NAME	5	AUTHORITY	6	DATA	7	GRPACC	Byte 1		0	NOGRPACC	1	UACC	2	ADSP	3	NOADSP	4	OWNER	5	SPECIAL	6	NOSPECIAL	7	OPERATIONS	Byte 2		0	NOOPERATIONS	1	CLAUTH	2	NOCLAUTH	3	AUDITOR	4	NOAUDITOR	5	OIDCARD	6	NOOIDCARD	*7	REVOKE	Byte 3		*0	RESUME	*1	AUDIT	*2	NOAUDIT	3	MODEL	*4	NOMODEL	5	WHEN	6	ADDCATEGORY	7	DELCATEGORY
Bit	Keyword Specified																																																																													
Byte 0																																																																														
0	DFLTGRP																																																																													
*1	GROUP																																																																													
2	PASSWORD																																																																													
3	NOPASSWORD																																																																													
4	NAME																																																																													
5	AUTHORITY																																																																													
6	DATA																																																																													
7	GRPACC																																																																													
Byte 1																																																																														
0	NOGRPACC																																																																													
1	UACC																																																																													
2	ADSP																																																																													
3	NOADSP																																																																													
4	OWNER																																																																													
5	SPECIAL																																																																													
6	NOSPECIAL																																																																													
7	OPERATIONS																																																																													
Byte 2																																																																														
0	NOOPERATIONS																																																																													
1	CLAUTH																																																																													
2	NOCLAUTH																																																																													
3	AUDITOR																																																																													
4	NOAUDITOR																																																																													
5	OIDCARD																																																																													
6	NOOIDCARD																																																																													
*7	REVOKE																																																																													
Byte 3																																																																														
*0	RESUME																																																																													
*1	AUDIT																																																																													
*2	NOAUDIT																																																																													
3	MODEL																																																																													
*4	NOMODEL																																																																													
5	WHEN																																																																													
6	ADDCATEGORY																																																																													
7	DELCATEGORY																																																																													
		4	Binary	Flags for keywords ignored because of insufficient authority: Same format as flags for keywords specified.																																																																										
		4	Binary	Flags for keywords ignored because of error conditions																																																																										
		1	Binary	Flags for other violations:																																																																										
				<table border="1"> <thead> <tr> <th>Bit</th> <th>Violation</th> </tr> </thead> <tbody> <tr> <td>*0</td> <td>Command invoker does not have CLAUTH attribute of USER</td> </tr> <tr> <td>1</td> <td>Command invoker does not have sufficient authority to group</td> </tr> <tr> <td>*2</td> <td>Command invoker does not have sufficient authority to user profile</td> </tr> <tr> <td>*3-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Violation	*0	Command invoker does not have CLAUTH attribute of USER	1	Command invoker does not have sufficient authority to group	*2	Command invoker does not have sufficient authority to user profile	*3-7	Reserved																																																																
Bit	Violation																																																																													
*0	Command invoker does not have CLAUTH attribute of USER																																																																													
1	Command invoker does not have sufficient authority to group																																																																													
*2	Command invoker does not have sufficient authority to user profile																																																																													
*3-7	Reserved																																																																													
		8	EBCDIC	User ID																																																																										
		8	EBCDIC	Group name (DFLTGRP keyword)																																																																										
		8	EBCDIC	*Group name (GROUP keyword)																																																																										

Event Code Dec(Hex)	Command	Data Length	Format	Description																						
10(A) (Cont.)	ADDUSER (Cont.)	1	Binary	Flags for AUTHORITY keyword: <table border="0"> <tr> <td>Bit</td> <td>Authority specified</td> </tr> <tr> <td>0</td> <td>JOIN</td> </tr> <tr> <td>1</td> <td>CONNECT</td> </tr> <tr> <td>2</td> <td>CREATE</td> </tr> <tr> <td>3</td> <td>USE</td> </tr> <tr> <td>4-7</td> <td>Reserved</td> </tr> </table>	Bit	Authority specified	0	JOIN	1	CONNECT	2	CREATE	3	USE	4-7	Reserved										
		Bit	Authority specified																							
		0	JOIN																							
		1	CONNECT																							
		2	CREATE																							
		3	USE																							
		4-7	Reserved																							
1	Binary	Flags for UACC keyword: <table border="0"> <tr> <td>Bit</td> <td>Authority Specified</td> </tr> <tr> <td>0</td> <td>ALTER</td> </tr> <tr> <td>1</td> <td>CONTROL</td> </tr> <tr> <td>2</td> <td>UPDATE</td> </tr> <tr> <td>3</td> <td>READ</td> </tr> <tr> <td>4-6</td> <td>Reserved</td> </tr> <tr> <td>7</td> <td>NONE</td> </tr> </table>	Bit	Authority Specified	0	ALTER	1	CONTROL	2	UPDATE	3	READ	4-6	Reserved	7	NONE										
Bit	Authority Specified																									
0	ALTER																									
1	CONTROL																									
2	UPDATE																									
3	READ																									
4-6	Reserved																									
7	NONE																									
8	EBCDIC	User ID or group name (OWNER keyword)																								
2	Binary	Flags for classes specified (CLAUTH keyword) <table border="0"> <tr> <td>Bit</td> <td>Option Specified</td> </tr> <tr> <td colspan="2">Byte 0</td> </tr> <tr> <td>0-1</td> <td>Reserved</td> </tr> <tr> <td>2</td> <td>USER</td> </tr> <tr> <td>3</td> <td>Reserved</td> </tr> <tr> <td>4</td> <td>DASDVOL</td> </tr> <tr> <td>5</td> <td>TAPEVOL</td> </tr> <tr> <td>6</td> <td>TERMINAL</td> </tr> <tr> <td>7</td> <td>Reserved</td> </tr> <tr> <td colspan="2">Byte 1</td> </tr> <tr> <td>0-7</td> <td>Reserved</td> </tr> </table>	Bit	Option Specified	Byte 0		0-1	Reserved	2	USER	3	Reserved	4	DASDVOL	5	TAPEVOL	6	TERMINAL	7	Reserved	Byte 1		0-7	Reserved		
Bit	Option Specified																									
Byte 0																										
0-1	Reserved																									
2	USER																									
3	Reserved																									
4	DASDVOL																									
5	TAPEVOL																									
6	TERMINAL																									
7	Reserved																									
Byte 1																										
0-7	Reserved																									
2	Binary	Flags for classes ignored because of insufficient authority: Same format as flags for classes specified. Note: if all classes specified are ignored because of insufficient authority, then the 'flags for keywords ignored because of insufficient authority' field indicates that CLAUTH was ignored.																								
2	Binary	Flags for additional keywords specified: <table border="0"> <tr> <td>Bit</td> <td>Keyword Specified</td> </tr> <tr> <td colspan="2">Byte 0</td> </tr> <tr> <td>0</td> <td>SECLEVEL</td> </tr> <tr> <td>1</td> <td>NOSECLEVEL</td> </tr> <tr> <td>2</td> <td>SECLABEL</td> </tr> <tr> <td>3</td> <td>NOSECLABEL</td> </tr> <tr> <td>4</td> <td>Reserved</td> </tr> <tr> <td>5</td> <td>Reserved</td> </tr> <tr> <td>6</td> <td>RESTRICTED</td> </tr> <tr> <td>7</td> <td>NORESTRICTED</td> </tr> <tr> <td colspan="2">Byte 1</td> </tr> <tr> <td>0-7</td> <td>Reserved</td> </tr> </table>	Bit	Keyword Specified	Byte 0		0	SECLEVEL	1	NOSECLEVEL	2	SECLABEL	3	NOSECLABEL	4	Reserved	5	Reserved	6	RESTRICTED	7	NORESTRICTED	Byte 1		0-7	Reserved
Bit	Keyword Specified																									
Byte 0																										
0	SECLEVEL																									
1	NOSECLEVEL																									
2	SECLABEL																									
3	NOSECLABEL																									
4	Reserved																									
5	Reserved																									
6	RESTRICTED																									
7	NORESTRICTED																									
Byte 1																										
0-7	Reserved																									

Data Type 6

Event Code Dec(Hex)	Command	Data Length	Format	Description																								
10(A) (Cont.)	ADDUSER (Cont.)	2	Binary	Flags for additional keywords ignored (authorization): <table border="0"> <thead> <tr> <th>Bit</th> <th>Keyword Ignored</th> </tr> </thead> <tbody> <tr> <td colspan="2">Byte 0</td> </tr> <tr> <td>0</td> <td>SECLEVEL</td> </tr> <tr> <td>1</td> <td>NOSECLEVEL</td> </tr> <tr> <td>2</td> <td>SECLABEL</td> </tr> <tr> <td>3</td> <td>NOSECLABEL</td> </tr> <tr> <td>4</td> <td>Reserved</td> </tr> <tr> <td>5</td> <td>Reserved</td> </tr> <tr> <td>6</td> <td>RESTRICTED</td> </tr> <tr> <td>7</td> <td>NORESTRICTED</td> </tr> <tr> <td colspan="2">Byte 1</td> </tr> <tr> <td>0-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Keyword Ignored	Byte 0		0	SECLEVEL	1	NOSECLEVEL	2	SECLABEL	3	NOSECLABEL	4	Reserved	5	Reserved	6	RESTRICTED	7	NORESTRICTED	Byte 1		0-7	Reserved
Bit	Keyword Ignored																											
Byte 0																												
0	SECLEVEL																											
1	NOSECLEVEL																											
2	SECLABEL																											
3	NOSECLABEL																											
4	Reserved																											
5	Reserved																											
6	RESTRICTED																											
7	NORESTRICTED																											
Byte 1																												
0-7	Reserved																											
		2	Binary	Flags for additional keywords ignored because of processing error: <table border="0"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr> <td colspan="2">Byte 0</td> </tr> <tr> <td>0</td> <td>SECLEVEL</td> </tr> <tr> <td>1</td> <td>NOSECLEVEL</td> </tr> <tr> <td>2</td> <td>SECLABEL</td> </tr> <tr> <td>3</td> <td>NOSECLABEL</td> </tr> <tr> <td>4</td> <td>Reserved</td> </tr> <tr> <td>5</td> <td>Reserved</td> </tr> <tr> <td>6</td> <td>RESTRICTED</td> </tr> <tr> <td>7</td> <td>NORESTRICTED</td> </tr> <tr> <td colspan="2">Byte 1</td> </tr> <tr> <td>0-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Keyword Specified	Byte 0		0	SECLEVEL	1	NOSECLEVEL	2	SECLABEL	3	NOSECLABEL	4	Reserved	5	Reserved	6	RESTRICTED	7	NORESTRICTED	Byte 1		0-7	Reserved
Bit	Keyword Specified																											
Byte 0																												
0	SECLEVEL																											
1	NOSECLEVEL																											
2	SECLABEL																											
3	NOSECLABEL																											
4	Reserved																											
5	Reserved																											
6	RESTRICTED																											
7	NORESTRICTED																											
Byte 1																												
0-7	Reserved																											
		3	packed	Logon time (packed); if time is not specified, this field contains binary zeroes; if TIME(ANYTIME) is specified, this field contains X'F0F0F0'.																								
		3	packed	Logoff time (packed); if time is not specified, this field contains binary zeroes; if TIME(ANYTIME) is specified, this field contains X'F0F0F0'.																								
		1	Binary	Logon day <table border="0"> <thead> <tr> <th>Bit</th> <th>Days the user cannot log on</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Sunday</td> </tr> <tr> <td>1</td> <td>Monday</td> </tr> <tr> <td>2</td> <td>Tuesday</td> </tr> <tr> <td>3</td> <td>Wednesday</td> </tr> <tr> <td>4</td> <td>Thursday</td> </tr> <tr> <td>5</td> <td>Friday</td> </tr> <tr> <td>6</td> <td>Saturday</td> </tr> <tr> <td>7</td> <td>Day not specified</td> </tr> </tbody> </table>	Bit	Days the user cannot log on	0	Sunday	1	Monday	2	Tuesday	3	Wednesday	4	Thursday	5	Friday	6	Saturday	7	Day not specified						
Bit	Days the user cannot log on																											
0	Sunday																											
1	Monday																											
2	Tuesday																											
3	Wednesday																											
4	Thursday																											
5	Friday																											
6	Saturday																											
7	Day not specified																											
		4	EBCDIC	REVOKE date																								
		4	EBCDIC	RESUME date																								
		44	EBCDIC	SECLEVEL name																								
		8	EBCDIC	SECLABEL name																								

Event Code Dec(Hex)	Command	Data Length	Format	Description																																				
11(B)	ALTDSD	2	Binary	Flags for keywords specified: <table border="0"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr> <td colspan="2">Byte 0</td> </tr> <tr> <td>0</td> <td>OWNER</td> </tr> <tr> <td>1</td> <td>UACC</td> </tr> <tr> <td>2</td> <td>AUDIT</td> </tr> <tr> <td>3</td> <td>LEVEL</td> </tr> <tr> <td>4</td> <td>ADDVOL</td> </tr> <tr> <td>5</td> <td>DELVOL</td> </tr> <tr> <td>6</td> <td>SET</td> </tr> <tr> <td>7</td> <td>NOSET</td> </tr> <tr> <td colspan="2">Byte 1</td> </tr> <tr> <td>0</td> <td>GLOBALAUDIT</td> </tr> <tr> <td>1</td> <td>VOLUME</td> </tr> <tr> <td>2</td> <td>PASSWORD</td> </tr> <tr> <td>3</td> <td>UNIT</td> </tr> <tr> <td>4</td> <td>ALTVOL</td> </tr> <tr> <td>5</td> <td>DATA</td> </tr> <tr> <td>6-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Keyword Specified	Byte 0		0	OWNER	1	UACC	2	AUDIT	3	LEVEL	4	ADDVOL	5	DELVOL	6	SET	7	NOSET	Byte 1		0	GLOBALAUDIT	1	VOLUME	2	PASSWORD	3	UNIT	4	ALTVOL	5	DATA	6-7	Reserved
Bit	Keyword Specified																																							
Byte 0																																								
0	OWNER																																							
1	UACC																																							
2	AUDIT																																							
3	LEVEL																																							
4	ADDVOL																																							
5	DELVOL																																							
6	SET																																							
7	NOSET																																							
Byte 1																																								
0	GLOBALAUDIT																																							
1	VOLUME																																							
2	PASSWORD																																							
3	UNIT																																							
4	ALTVOL																																							
5	DATA																																							
6-7	Reserved																																							
		2	Binary	Flags for keywords ignored because of insufficient authority: Same format as flags for keywords specified, except that Byte 1, Bit 2 is reserved.																																				
		2	Binary	Flags for keywords ignored because of error conditions: Same format as flags for keywords specified, except that Byte 1, Bit 2 is reserved.																																				
		44	EBCDIC	Data set name																																				
		8	EBCDIC	User ID or group name (OWNER keyword)																																				
		1	Binary	Flags for UACC keyword: Note: If this is a non-DFP data set, RACF ignores bit 4 when checking access to the data set. <table border="0"> <thead> <tr> <th>Bit</th> <th>Authority Specified</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>ALTER</td> </tr> <tr> <td>1</td> <td>CONTROL</td> </tr> <tr> <td>2</td> <td>UPDATE</td> </tr> <tr> <td>3</td> <td>READ</td> </tr> <tr> <td>4</td> <td>EXECUTE</td> </tr> <tr> <td>5-6</td> <td>Reserved</td> </tr> <tr> <td>7</td> <td>NONE</td> </tr> </tbody> </table>	Bit	Authority Specified	0	ALTER	1	CONTROL	2	UPDATE	3	READ	4	EXECUTE	5-6	Reserved	7	NONE																				
Bit	Authority Specified																																							
0	ALTER																																							
1	CONTROL																																							
2	UPDATE																																							
3	READ																																							
4	EXECUTE																																							
5-6	Reserved																																							
7	NONE																																							
		1	Binary	Flags for AUDIT keyword: <table border="0"> <thead> <tr> <th>Bit</th> <th>Option Specified</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>ALL</td> </tr> <tr> <td>1</td> <td>SUCCESS</td> </tr> <tr> <td>2</td> <td>FAILURES</td> </tr> <tr> <td>3</td> <td>NONE</td> </tr> <tr> <td>4-5</td> <td>SUCCESS qualifier codes</td> </tr> <tr> <td>6-7</td> <td>FAILURES qualifier codes</td> </tr> </tbody> </table>	Bit	Option Specified	0	ALL	1	SUCCESS	2	FAILURES	3	NONE	4-5	SUCCESS qualifier codes	6-7	FAILURES qualifier codes																						
Bit	Option Specified																																							
0	ALL																																							
1	SUCCESS																																							
2	FAILURES																																							
3	NONE																																							
4-5	SUCCESS qualifier codes																																							
6-7	FAILURES qualifier codes																																							
		1	Binary	nn (LEVEL keyword)																																				
		1	Binary	Flags for GLOBALAUDIT keyword: Same format as flags for AUDIT keyword.																																				
		6	EBCDIC	Volume serial ID (VOLUME keyword)																																				

Data Type 6

Event Code Dec(Hex)	Command	Data Length	Format	Description	
11(B) (Cont.)	ALTDSD (Cont.)	8	EBCDIC	Unit information	
		1	Binary	Flags for RACF processing:	
				Bit	Meaning
				0	Profile inconsistent with RACF indicator.
				1	Generic profile name specified
				2-7	Reserved
		2	Binary	Additional keywords specified:	
				Bit	Keyword Specified
				Byte 0	
				0	GENERIC
				1	WARNING
				2	NOWARNING
				3	ERASE
				4	NOERASE
		5	RETPD		
		6	NOTIFY		
		7	NONOTIFY		
		Byte 1			
		0	SECLEVEL		
		1	ADDCATEGORY		
		2	DELCATEGORY		
		3	NOSECLEVEL		
		4	SECLABEL		
		5	NOSECLABEL		
		6-7	Reserved		
2	Binary	Flags for keywords ignored because of insufficient authority: Same format as flags for keywords specified.			
2	Binary	Flags for keywords ignored because of a processing error: Same format as flags for keywords specified.			
2	Binary	Retention period			
8	EBCDIC	User to be notified when access denied.			
44	EBCDIC	SECLEVEL name			
8	EBCDIC	SECLABEL name			
12(C)	ALTRGROUP	1	Binary	Flags for keywords specified:	
				Bit	Keyword Specified
				0	SUPGROUP
				1	OWNER
				2	NOTERMUACC
				3	TERMUACC
				4	DATA
				5	MODEL
				6-7	Reserved
		1	Binary	Flags for keywords ignored because of insufficient authority: Same format as flags for keyword's specified.	
		1	Binary	Flags for other violations:	
		Bit	Violation		
		0	Lack of proper authority to old SUPGROUP		
		1-7	Reserved		
8	EBCDIC	Group name			
8	EBCDIC	Superior group name (SUPGROUP keyword)			
8	EBCDIC	User ID or group name (OWNER keyword)			
1	Binary	Flags for keywords ignored because of error conditions: Same format as flags for keywords specified.			

Event Code Dec(Hex)	Command	Data Length	Format	Description																																																																										
13(D)	ALTUSER	* The data for event code 13 is identical to the data for event code 10, with these exceptions.																																																																												
		4	Binary	Flags for keywords specified:																																																																										
				<table border="1"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr> <td colspan="2">Byte 0</td> </tr> <tr> <td>0</td> <td>DFLTGRP</td> </tr> <tr> <td>*1</td> <td>GROUP</td> </tr> <tr> <td>2</td> <td>PASSWORD</td> </tr> <tr> <td>3</td> <td>NOPASSWORD</td> </tr> <tr> <td>4</td> <td>NAME</td> </tr> <tr> <td>5</td> <td>AUTHORITY</td> </tr> <tr> <td>6</td> <td>DATA</td> </tr> <tr> <td>7</td> <td>GRPACC</td> </tr> <tr> <td colspan="2">Byte 1</td> </tr> <tr> <td>0</td> <td>NOGRPACC</td> </tr> <tr> <td>1</td> <td>UACC</td> </tr> <tr> <td>2</td> <td>ADSP</td> </tr> <tr> <td>3</td> <td>NOADSP</td> </tr> <tr> <td>4</td> <td>OWNER</td> </tr> <tr> <td>5</td> <td>SPECIAL</td> </tr> <tr> <td>6</td> <td>NOSPECIAL</td> </tr> <tr> <td>7</td> <td>OPERATIONS</td> </tr> <tr> <td colspan="2">Byte 2</td> </tr> <tr> <td>0</td> <td>NOOPERATIONS</td> </tr> <tr> <td>1</td> <td>CLAUTH</td> </tr> <tr> <td>2</td> <td>NOCLAUTH</td> </tr> <tr> <td>3</td> <td>AUDITOR</td> </tr> <tr> <td>4</td> <td>NOAUDITOR</td> </tr> <tr> <td>5</td> <td>OIDCARD</td> </tr> <tr> <td>6</td> <td>NOOIDCARD</td> </tr> <tr> <td>*7</td> <td>REVOKE</td> </tr> <tr> <td colspan="2">Byte 3</td> </tr> <tr> <td>*0</td> <td>RESUME</td> </tr> <tr> <td>*1</td> <td>UAUDIT</td> </tr> <tr> <td>*2</td> <td>NOUAUDIT</td> </tr> <tr> <td>3</td> <td>MODEL</td> </tr> <tr> <td>4</td> <td>NOMODEL</td> </tr> <tr> <td>5</td> <td>WHEN</td> </tr> <tr> <td>6</td> <td>ADDCATEGORY</td> </tr> <tr> <td>7</td> <td>DELCATEGORY</td> </tr> </tbody> </table>	Bit	Keyword Specified	Byte 0		0	DFLTGRP	*1	GROUP	2	PASSWORD	3	NOPASSWORD	4	NAME	5	AUTHORITY	6	DATA	7	GRPACC	Byte 1		0	NOGRPACC	1	UACC	2	ADSP	3	NOADSP	4	OWNER	5	SPECIAL	6	NOSPECIAL	7	OPERATIONS	Byte 2		0	NOOPERATIONS	1	CLAUTH	2	NOCLAUTH	3	AUDITOR	4	NOAUDITOR	5	OIDCARD	6	NOOIDCARD	*7	REVOKE	Byte 3		*0	RESUME	*1	UAUDIT	*2	NOUAUDIT	3	MODEL	4	NOMODEL	5	WHEN	6	ADDCATEGORY	7	DELCATEGORY
Bit	Keyword Specified																																																																													
Byte 0																																																																														
0	DFLTGRP																																																																													
*1	GROUP																																																																													
2	PASSWORD																																																																													
3	NOPASSWORD																																																																													
4	NAME																																																																													
5	AUTHORITY																																																																													
6	DATA																																																																													
7	GRPACC																																																																													
Byte 1																																																																														
0	NOGRPACC																																																																													
1	UACC																																																																													
2	ADSP																																																																													
3	NOADSP																																																																													
4	OWNER																																																																													
5	SPECIAL																																																																													
6	NOSPECIAL																																																																													
7	OPERATIONS																																																																													
Byte 2																																																																														
0	NOOPERATIONS																																																																													
1	CLAUTH																																																																													
2	NOCLAUTH																																																																													
3	AUDITOR																																																																													
4	NOAUDITOR																																																																													
5	OIDCARD																																																																													
6	NOOIDCARD																																																																													
*7	REVOKE																																																																													
Byte 3																																																																														
*0	RESUME																																																																													
*1	UAUDIT																																																																													
*2	NOUAUDIT																																																																													
3	MODEL																																																																													
4	NOMODEL																																																																													
5	WHEN																																																																													
6	ADDCATEGORY																																																																													
7	DELCATEGORY																																																																													
		4	Binary	Flags for keywords ignored because of insufficient authority: Same format as flags for keywords specified.																																																																										
		4	Binary	Flags for keywords ignored because of error conditions: Same format as flags for keywords specified.																																																																										
		1	Binary	Flags for other violations:																																																																										
				<table border="1"> <thead> <tr> <th>Bit</th> <th>Violation</th> </tr> </thead> <tbody> <tr> <td>*0</td> <td>Command invoker does not have CLAUTH attribute of USER</td> </tr> <tr> <td>1</td> <td>Command invoker does not have sufficient authority to group</td> </tr> <tr> <td>*2</td> <td>Command invoker does not have sufficient authority to user profile</td> </tr> <tr> <td>3</td> <td>Reserved</td> </tr> <tr> <td>4</td> <td>NOEXPIRED</td> </tr> <tr> <td>5</td> <td>EXPIRED</td> </tr> <tr> <td>6-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Violation	*0	Command invoker does not have CLAUTH attribute of USER	1	Command invoker does not have sufficient authority to group	*2	Command invoker does not have sufficient authority to user profile	3	Reserved	4	NOEXPIRED	5	EXPIRED	6-7	Reserved																																																										
Bit	Violation																																																																													
*0	Command invoker does not have CLAUTH attribute of USER																																																																													
1	Command invoker does not have sufficient authority to group																																																																													
*2	Command invoker does not have sufficient authority to user profile																																																																													
3	Reserved																																																																													
4	NOEXPIRED																																																																													
5	EXPIRED																																																																													
6-7	Reserved																																																																													

Data Type 6

Event Code Dec(Hex)	Command	Data Length	Format	Description																						
13(D) (Cont.)	ALTUSER (Cont.)	8	EBCDIC	User ID																						
		8	EBCDIC	Group name (DFLTGRP keyword)																						
		8	EBCDIC	*Group name (GROUP keyword)																						
		1	Binary	Flags for AUTHORITY keyword: <table border="0"> <thead> <tr> <th>Bit</th> <th>Authority Specified</th> </tr> </thead> <tbody> <tr><td>0</td><td>JOIN</td></tr> <tr><td>1</td><td>CONNECT</td></tr> <tr><td>2</td><td>CREATE</td></tr> <tr><td>3</td><td>USE</td></tr> <tr><td>4-7</td><td>Reserved</td></tr> </tbody> </table>	Bit	Authority Specified	0	JOIN	1	CONNECT	2	CREATE	3	USE	4-7	Reserved										
		Bit	Authority Specified																							
		0	JOIN																							
		1	CONNECT																							
		2	CREATE																							
		3	USE																							
		4-7	Reserved																							
1	Binary	Flags for UACC keyword: <table border="0"> <thead> <tr> <th>Bit</th> <th>Authority Specified</th> </tr> </thead> <tbody> <tr><td>0</td><td>ALTER</td></tr> <tr><td>1</td><td>CONTROL</td></tr> <tr><td>2</td><td>UPDATE</td></tr> <tr><td>3</td><td>READ</td></tr> <tr><td>4-6</td><td>Reserved</td></tr> <tr><td>7</td><td>NONE</td></tr> </tbody> </table>	Bit	Authority Specified	0	ALTER	1	CONTROL	2	UPDATE	3	READ	4-6	Reserved	7	NONE										
Bit	Authority Specified																									
0	ALTER																									
1	CONTROL																									
2	UPDATE																									
3	READ																									
4-6	Reserved																									
7	NONE																									
8	EBCDIC	User ID (OWNER keyword)																								
2	Binary	Flags for classes specified (CLAUTH keywords) <table border="0"> <thead> <tr> <th>Bit</th> <th>Option Specified</th> </tr> </thead> <tbody> <tr><td colspan="2">Byte 0</td></tr> <tr><td>0-1</td><td>Reserved</td></tr> <tr><td>2</td><td>USER</td></tr> <tr><td>3</td><td>Reserved</td></tr> <tr><td>4</td><td>DASDVOL</td></tr> <tr><td>5</td><td>TAPEVOL</td></tr> <tr><td>6</td><td>TERMINAL</td></tr> <tr><td>7</td><td>Reserved</td></tr> <tr><td colspan="2">Byte 1</td></tr> <tr><td>0-7</td><td>Reserved</td></tr> </tbody> </table>	Bit	Option Specified	Byte 0		0-1	Reserved	2	USER	3	Reserved	4	DASDVOL	5	TAPEVOL	6	TERMINAL	7	Reserved	Byte 1		0-7	Reserved		
Bit	Option Specified																									
Byte 0																										
0-1	Reserved																									
2	USER																									
3	Reserved																									
4	DASDVOL																									
5	TAPEVOL																									
6	TERMINAL																									
7	Reserved																									
Byte 1																										
0-7	Reserved																									
2	Binary	Flags for classes ignored because of insufficient authority: Same format as flags for classes specified. <p>Note that if all classes specified are ignored because of insufficient authority, then the 'flags for keywords ignored because of insufficient authority' field indicates that CLAUTH or NOCLAUTH was ignored.</p>																								
2	Binary	Flags for additional keywords specified: <table border="0"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr><td colspan="2">Byte 0</td></tr> <tr><td>0</td><td>SECLEVEL</td></tr> <tr><td>*1</td><td>NOSECLEVEL</td></tr> <tr><td>*2</td><td>SECLABEL</td></tr> <tr><td>*3</td><td>NOSECLABEL</td></tr> <tr><td>*4</td><td>NOEXPIRED</td></tr> <tr><td>*5</td><td>EXPIRED</td></tr> <tr><td>*6</td><td>RESTRICTED</td></tr> <tr><td>*7</td><td>NORESTRICTED</td></tr> <tr><td colspan="2">Byte 1</td></tr> <tr><td>0-7</td><td>Reserved</td></tr> </tbody> </table>	Bit	Keyword Specified	Byte 0		0	SECLEVEL	*1	NOSECLEVEL	*2	SECLABEL	*3	NOSECLABEL	*4	NOEXPIRED	*5	EXPIRED	*6	RESTRICTED	*7	NORESTRICTED	Byte 1		0-7	Reserved
Bit	Keyword Specified																									
Byte 0																										
0	SECLEVEL																									
*1	NOSECLEVEL																									
*2	SECLABEL																									
*3	NOSECLABEL																									
*4	NOEXPIRED																									
*5	EXPIRED																									
*6	RESTRICTED																									
*7	NORESTRICTED																									
Byte 1																										
0-7	Reserved																									

Event Code Dec(Hex)	Command	Data Length	Format	Description																								
13(D) (Cont.)	ALTUSER (Cont.)	2	Binary	Flags for additional keywords ignored (authorization): <table border="0"> <thead> <tr> <th>Bit</th> <th>Keyword Ignored</th> </tr> </thead> <tbody> <tr> <td colspan="2">Byte 0</td> </tr> <tr> <td>0</td> <td>SECLEVEL</td> </tr> <tr> <td>*1</td> <td>NOSECLEVEL</td> </tr> <tr> <td>*2</td> <td>SECLABEL</td> </tr> <tr> <td>*3</td> <td>NOSECLABEL</td> </tr> <tr> <td>*4</td> <td>NOEXPIRED</td> </tr> <tr> <td>*5</td> <td>EXPIRED</td> </tr> <tr> <td>*6</td> <td>RESTRICTED</td> </tr> <tr> <td>*7</td> <td>NORESTRICTED</td> </tr> <tr> <td colspan="2">Byte 1</td> </tr> <tr> <td>0-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Keyword Ignored	Byte 0		0	SECLEVEL	*1	NOSECLEVEL	*2	SECLABEL	*3	NOSECLABEL	*4	NOEXPIRED	*5	EXPIRED	*6	RESTRICTED	*7	NORESTRICTED	Byte 1		0-7	Reserved
Bit	Keyword Ignored																											
Byte 0																												
0	SECLEVEL																											
*1	NOSECLEVEL																											
*2	SECLABEL																											
*3	NOSECLABEL																											
*4	NOEXPIRED																											
*5	EXPIRED																											
*6	RESTRICTED																											
*7	NORESTRICTED																											
Byte 1																												
0-7	Reserved																											
		2	Binary	Flags for additional keywords ignored because of processing error: <table border="0"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr> <td colspan="2">Byte 0</td> </tr> <tr> <td>0</td> <td>SECLEVEL</td> </tr> <tr> <td>*1</td> <td>NOSECLEVEL</td> </tr> <tr> <td>*2</td> <td>SECLABEL</td> </tr> <tr> <td>*3</td> <td>NOSECLABEL</td> </tr> <tr> <td>*4</td> <td>NOEXPIRED</td> </tr> <tr> <td>*5</td> <td>EXPIRED</td> </tr> <tr> <td>*6</td> <td>RESTRICTED</td> </tr> <tr> <td>*7</td> <td>NORESTRICTED</td> </tr> <tr> <td colspan="2">Byte 1</td> </tr> <tr> <td>0-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Keyword Specified	Byte 0		0	SECLEVEL	*1	NOSECLEVEL	*2	SECLABEL	*3	NOSECLABEL	*4	NOEXPIRED	*5	EXPIRED	*6	RESTRICTED	*7	NORESTRICTED	Byte 1		0-7	Reserved
Bit	Keyword Specified																											
Byte 0																												
0	SECLEVEL																											
*1	NOSECLEVEL																											
*2	SECLABEL																											
*3	NOSECLABEL																											
*4	NOEXPIRED																											
*5	EXPIRED																											
*6	RESTRICTED																											
*7	NORESTRICTED																											
Byte 1																												
0-7	Reserved																											
		3	packed	Logon time (packed); if time is not specified, this field contains binary zeroes; if TIME(ANYTIME) is specified, this field contains X'F0F0F0'.																								
		3	packed	Logoff time (packed); if time is not specified, this field contains binary zeroes; if TIME(ANYTIME) is specified, this field contains X'F0F0F0'.																								
		1	Binary	Day(s) the user cannot logon <table border="0"> <thead> <tr> <th>Bit</th> <th>Day Specified</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Sunday</td> </tr> <tr> <td>1</td> <td>Monday</td> </tr> <tr> <td>2</td> <td>Tuesday</td> </tr> <tr> <td>3</td> <td>Wednesday</td> </tr> <tr> <td>4</td> <td>Thursday</td> </tr> <tr> <td>5</td> <td>Friday</td> </tr> <tr> <td>6</td> <td>Saturday</td> </tr> <tr> <td>7</td> <td>Day not specified</td> </tr> </tbody> </table>	Bit	Day Specified	0	Sunday	1	Monday	2	Tuesday	3	Wednesday	4	Thursday	5	Friday	6	Saturday	7	Day not specified						
Bit	Day Specified																											
0	Sunday																											
1	Monday																											
2	Tuesday																											
3	Wednesday																											
4	Thursday																											
5	Friday																											
6	Saturday																											
7	Day not specified																											
		4	EBCDIC	REVOKE date																								
		4	EBCDIC	RESUME date																								
		44	EBCDIC	SECLEVEL name																								
		8	EBCDIC	SECLABEL name																								

Data Type 6

Event Code Dec(Hex)	Command	Data Length	Format	Description																																				
14(E)	CONNECT	2	Binary	Flags for keywords specified:																																				
				<table border="1"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr> <td colspan="2">Byte 0</td> </tr> <tr> <td>0</td> <td>GROUP</td> </tr> <tr> <td>1</td> <td>UACC</td> </tr> <tr> <td>2</td> <td>AUTHORITY</td> </tr> <tr> <td>3</td> <td>ADSP</td> </tr> <tr> <td>4</td> <td>NOADSP</td> </tr> <tr> <td>5</td> <td>REVOKE</td> </tr> <tr> <td>6</td> <td>RESUME</td> </tr> <tr> <td>7</td> <td>GRPACC</td> </tr> <tr> <td colspan="2">Byte 1</td> </tr> <tr> <td>0</td> <td>NOGRPACC</td> </tr> <tr> <td>1</td> <td>OPERATIONS</td> </tr> <tr> <td>2</td> <td>NOOPERATIONS</td> </tr> <tr> <td>3</td> <td>SPECIAL</td> </tr> <tr> <td>4</td> <td>NOSPECIAL</td> </tr> <tr> <td>5</td> <td>AUDITOR</td> </tr> <tr> <td>6</td> <td>NOAUDITOR</td> </tr> <tr> <td>7</td> <td>OWNER</td> </tr> </tbody> </table>	Bit	Keyword Specified	Byte 0		0	GROUP	1	UACC	2	AUTHORITY	3	ADSP	4	NOADSP	5	REVOKE	6	RESUME	7	GRPACC	Byte 1		0	NOGRPACC	1	OPERATIONS	2	NOOPERATIONS	3	SPECIAL	4	NOSPECIAL	5	AUDITOR	6	NOAUDITOR
		Bit	Keyword Specified																																					
		Byte 0																																						
		0	GROUP																																					
		1	UACC																																					
		2	AUTHORITY																																					
		3	ADSP																																					
		4	NOADSP																																					
		5	REVOKE																																					
		6	RESUME																																					
		7	GRPACC																																					
		Byte 1																																						
		0	NOGRPACC																																					
1	OPERATIONS																																							
2	NOOPERATIONS																																							
3	SPECIAL																																							
4	NOSPECIAL																																							
5	AUDITOR																																							
6	NOAUDITOR																																							
7	OWNER																																							
2	Binary	Flags for keywords ignored because of insufficient authority: Same format as flags for keywords specified.																																						
8	EBCDIC	User ID																																						
8	EBCDIC	Group name (GROUP keyword)																																						
1	Binary	Flags for UACC keyword:																																						
		<table border="1"> <thead> <tr> <th>Bit</th> <th>Authority Specified</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>ALTER</td> </tr> <tr> <td>1</td> <td>CONTROL</td> </tr> <tr> <td>2</td> <td>UPDATE</td> </tr> <tr> <td>3</td> <td>READ</td> </tr> <tr> <td>4-6</td> <td>Reserved</td> </tr> <tr> <td>7</td> <td>NONE</td> </tr> </tbody> </table>	Bit	Authority Specified	0	ALTER	1	CONTROL	2	UPDATE	3	READ	4-6	Reserved	7	NONE																								
Bit	Authority Specified																																							
0	ALTER																																							
1	CONTROL																																							
2	UPDATE																																							
3	READ																																							
4-6	Reserved																																							
7	NONE																																							
1	Binary	Flags for AUTHORITY keyword:																																						
		<table border="1"> <thead> <tr> <th>Bit</th> <th>Authority Specified</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>JOIN</td> </tr> <tr> <td>1</td> <td>CONNECT</td> </tr> <tr> <td>2</td> <td>CREATE</td> </tr> <tr> <td>3</td> <td>USE</td> </tr> <tr> <td>4-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Authority Specified	0	JOIN	1	CONNECT	2	CREATE	3	USE	4-7	Reserved																										
Bit	Authority Specified																																							
0	JOIN																																							
1	CONNECT																																							
2	CREATE																																							
3	USE																																							
4-7	Reserved																																							
2	EBCDIC	Reserved																																						
8	EBCDIC	User ID or group name (OWNER keyword)																																						
4	packed	REVOKE date, packed																																						
4	packed	RESUME date, packed																																						
15(F)	DELDSD	1	Binary	Flags for keywords specified or taken as defaults:																																				
				<table border="1"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>SET</td> </tr> <tr> <td>1</td> <td>NOSET</td> </tr> <tr> <td>2</td> <td>VOLUME</td> </tr> <tr> <td>3</td> <td>GENERIC</td> </tr> <tr> <td>4-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Keyword Specified	0	SET	1	NOSET	2	VOLUME	3	GENERIC	4-7	Reserved																								
		Bit	Keyword Specified																																					
		0	SET																																					
		1	NOSET																																					
		2	VOLUME																																					
		3	GENERIC																																					
4-7	Reserved																																							
1	Binary	Flags for keywords ignored because of insufficient authority: Same format as flags for keywords specified.																																						
44	EBCDIC	Data set name																																						
6	EBCDIC	Volume serial ID (VOLUME keyword)																																						
1	Binary	Flags for RACF processing:																																						
		<table border="1"> <thead> <tr> <th>Bit</th> <th>Meaning</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Profile inconsistent with RACF indicator</td> </tr> <tr> <td>1</td> <td>Generic profile name specified</td> </tr> <tr> <td>2-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Meaning	0	Profile inconsistent with RACF indicator	1	Generic profile name specified	2-7	Reserved																														
Bit	Meaning																																							
0	Profile inconsistent with RACF indicator																																							
1	Generic profile name specified																																							
2-7	Reserved																																							

Event Code Dec(Hex)	Command	Data Length	Format	Description	
16(10)	DELGROUP	8	EBCDIC	Group name	
17(11)	DELUSER	8	EBCDIC	User ID	
18(12)	PASSWORD	1	Binary	Flags for keywords specified:	
				Bit	Keyword Specified
				0	INTERVAL
				1	USER
				2	PASSWORD
				3-7	Reserved
				1	Binary
1	Binary	Flags for keywords ignored because of error conditions: Same format as flags for keywords specified.			
4	Binary	Change-interval (INTERVAL keyword) Note: If the NOINTERVAL keyword is specified, the change-interval changes to X'FF'.			
8	EBCDIC	User ID (USER keyword)			
19(13)	PERMIT	2	Binary	Flags for keywords specified or taken as defaults:	
				Bit	Keyword Specified
				Byte 0	
				0	CLASS
				1	ID
				2	ACCESS
				3	FROM
4	DELETE				
5	FCLASS				
6	VOLUME				
7	FVOLUME				
Byte 1					
0	GENERIC				
1	FGENERIC				
2	RESET				
3	WHEN				
4	RESET(WHEN)				
5	RESET(STANDARD)				
6-7	Reserved				
2	Binary	Flags for keywords ignored because of insufficient authority: Same format as flags for keywords specified, except that bits are not set for RESET(STANDARD) or RESET(WHEN).			
2	Binary	Flags for keywords ignored because of error conditions: Same format as flags for keywords specified, except that bits are not set for RESET(STANDARD) or RESET(WHEN).			
2	Binary	Flags for CLASS keyword, and for the RESET keyword:			
Bit	Option Specified				
Byte 0					
0-2	Reserved				
3	DATASET				
4	DASDVOL				
5	TAPEVOL				
6	TERMINAL				
7	Reserved				
Byte 1					
0	FROM generic resource				
1-5	Reserved				
6	Conditional access list is indicated by RESET keyword.				
7	Standard access list is indicated by RESET keyword.				

Data Type 6

Event Code Dec(Hex)	Command	Data Length	Format	Description																																						
19(13) (Cont.)	PERMIT (Cont.)	1	Binary	Flags for ACCESS keyword: Note: If this is a non-DFP data set, RACF ignores bit 4 when checking access to the data set.																																						
				<table border="0"> <thead> <tr> <th>Bit</th> <th>Authority Specified</th> </tr> </thead> <tbody> <tr><td>0</td><td>ALTER</td></tr> <tr><td>1</td><td>CONTROL</td></tr> <tr><td>2</td><td>UPDATE</td></tr> <tr><td>3</td><td>READ</td></tr> <tr><td>4</td><td>EXECUTE</td></tr> <tr><td>5-6</td><td>Reserved</td></tr> <tr><td>7</td><td>NONE</td></tr> </tbody> </table>	Bit	Authority Specified	0	ALTER	1	CONTROL	2	UPDATE	3	READ	4	EXECUTE	5-6	Reserved	7	NONE																						
Bit	Authority Specified																																									
0	ALTER																																									
1	CONTROL																																									
2	UPDATE																																									
3	READ																																									
4	EXECUTE																																									
5-6	Reserved																																									
7	NONE																																									
		2	Binary	Flags for FCLASS keyword: Same format as flags for CLASS keyword.																																						
20(14)	RALTER	* The data for event code 20 is identical with the data for event code 21, with these exceptions.																																								
		2	Binary	Flags for keywords specified:																																						
				<table border="0"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr><td colspan="2">Byte 0</td></tr> <tr><td>0</td><td>DATA</td></tr> <tr><td>1</td><td>OWNER</td></tr> <tr><td>2</td><td>UACC</td></tr> <tr><td>3</td><td>LEVEL</td></tr> <tr><td>4</td><td>AUDIT</td></tr> <tr><td>*5</td><td>GLOBALAUDIT</td></tr> <tr><td>*6</td><td>ADDVOL</td></tr> <tr><td>*7</td><td>DELVOL</td></tr> <tr><td colspan="2">Byte 1</td></tr> <tr><td>0</td><td>ADDMEM</td></tr> <tr><td>1</td><td>DELMEM</td></tr> <tr><td>2</td><td>APPLDATA</td></tr> <tr><td>3</td><td>SINGLEDSN</td></tr> <tr><td>*4</td><td>NOSINGLEDSN</td></tr> <tr><td>5</td><td>WARNING</td></tr> <tr><td>6</td><td>NOWARNING</td></tr> <tr><td>7</td><td>WHEN</td></tr> </tbody> </table>	Bit	Keyword Specified	Byte 0		0	DATA	1	OWNER	2	UACC	3	LEVEL	4	AUDIT	*5	GLOBALAUDIT	*6	ADDVOL	*7	DELVOL	Byte 1		0	ADDMEM	1	DELMEM	2	APPLDATA	3	SINGLEDSN	*4	NOSINGLEDSN	5	WARNING	6	NOWARNING	7	WHEN
Bit	Keyword Specified																																									
Byte 0																																										
0	DATA																																									
1	OWNER																																									
2	UACC																																									
3	LEVEL																																									
4	AUDIT																																									
*5	GLOBALAUDIT																																									
*6	ADDVOL																																									
*7	DELVOL																																									
Byte 1																																										
0	ADDMEM																																									
1	DELMEM																																									
2	APPLDATA																																									
3	SINGLEDSN																																									
*4	NOSINGLEDSN																																									
5	WARNING																																									
6	NOWARNING																																									
7	WHEN																																									
		2	Binary	Flags for keywords ignored because of insufficient authority: Same format as flags for keywords specified.																																						
		2	Binary	Flags for class name:																																						
				<table border="0"> <thead> <tr> <th>Bit</th> <th>Option Specified</th> </tr> </thead> <tbody> <tr><td colspan="2">Byte 0</td></tr> <tr><td>0-3</td><td>Reserved</td></tr> <tr><td>4</td><td>DASDVOL</td></tr> <tr><td>5</td><td>TAPEVOL</td></tr> <tr><td>6</td><td>TERMINAL</td></tr> <tr><td>7</td><td>Reserved</td></tr> <tr><td colspan="2">Byte 1</td></tr> <tr><td>0</td><td>Generic resource name specified.</td></tr> <tr><td>1-7</td><td>Reserved</td></tr> </tbody> </table>	Bit	Option Specified	Byte 0		0-3	Reserved	4	DASDVOL	5	TAPEVOL	6	TERMINAL	7	Reserved	Byte 1		0	Generic resource name specified.	1-7	Reserved																		
Bit	Option Specified																																									
Byte 0																																										
0-3	Reserved																																									
4	DASDVOL																																									
5	TAPEVOL																																									
6	TERMINAL																																									
7	Reserved																																									
Byte 1																																										
0	Generic resource name specified.																																									
1-7	Reserved																																									
		8	EBCDIC	User ID or group name (OWNER keyword)																																						
		1	Binary	Flags for UACC keyword:																																						
				<table border="0"> <thead> <tr> <th>Bit</th> <th>Authority Specified</th> </tr> </thead> <tbody> <tr><td>0</td><td>ALTER</td></tr> <tr><td>1</td><td>CONTROL</td></tr> <tr><td>2</td><td>UPDATE</td></tr> <tr><td>3</td><td>READ</td></tr> <tr><td>4</td><td>EXECUTE</td></tr> <tr><td>5-6</td><td>Reserved</td></tr> <tr><td>7</td><td>NONE</td></tr> </tbody> </table>	Bit	Authority Specified	0	ALTER	1	CONTROL	2	UPDATE	3	READ	4	EXECUTE	5-6	Reserved	7	NONE																						
Bit	Authority Specified																																									
0	ALTER																																									
1	CONTROL																																									
2	UPDATE																																									
3	READ																																									
4	EXECUTE																																									
5-6	Reserved																																									
7	NONE																																									
		1	Binary	nn (LEVEL keyword)																																						

Event Code Dec(Hex)	Command	Data Length	Format	Description																																						
20(14) (Cont.)	RALTER (Cont.)	1	Binary	Flags for AUDIT keyword: <table border="0"> <thead> <tr> <th>Bit</th> <th>Option Specified</th> </tr> </thead> <tbody> <tr><td>0</td><td>ALL</td></tr> <tr><td>1</td><td>SUCCESS</td></tr> <tr><td>2</td><td>FAILURES</td></tr> <tr><td>3</td><td>NONE</td></tr> <tr><td>4-5</td><td>Success qualifier codes:</td></tr> <tr><td></td><td>'00' — READ</td></tr> <tr><td></td><td>'01' — UPDATE</td></tr> <tr><td></td><td>'10' — CONTROL</td></tr> <tr><td></td><td>'11' — ALTER</td></tr> <tr><td>6-7</td><td>FAILURES qualifier codes:</td></tr> <tr><td></td><td>'00' — READ</td></tr> <tr><td></td><td>'01' — UPDATE</td></tr> <tr><td></td><td>'10' — CONTROL</td></tr> <tr><td></td><td>'11' — ALTER</td></tr> </tbody> </table>	Bit	Option Specified	0	ALL	1	SUCCESS	2	FAILURES	3	NONE	4-5	Success qualifier codes:		'00' — READ		'01' — UPDATE		'10' — CONTROL		'11' — ALTER	6-7	FAILURES qualifier codes:		'00' — READ		'01' — UPDATE		'10' — CONTROL		'11' — ALTER								
Bit	Option Specified																																									
0	ALL																																									
1	SUCCESS																																									
2	FAILURES																																									
3	NONE																																									
4-5	Success qualifier codes:																																									
	'00' — READ																																									
	'01' — UPDATE																																									
	'10' — CONTROL																																									
	'11' — ALTER																																									
6-7	FAILURES qualifier codes:																																									
	'00' — READ																																									
	'01' — UPDATE																																									
	'10' — CONTROL																																									
	'11' — ALTER																																									
		1	Binary	*Flags for GLOBALAUDIT keyword: Same format as flags for AUDIT keyword.																																						
		2	Binary	Flags for keywords specified: <table border="0"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr><td colspan="2">Byte 0</td></tr> <tr><td>0</td><td>NOTIFY</td></tr> <tr><td>*1</td><td>NONOTIFY</td></tr> <tr><td>2</td><td>TVTOC</td></tr> <tr><td>*3</td><td>NOTVTOC</td></tr> <tr><td>4</td><td>TIMEZONE</td></tr> <tr><td>*5</td><td>NOTIMEZONE</td></tr> <tr><td>6</td><td>ADDCATEGORY</td></tr> <tr><td>*7</td><td>DELCATEGORY</td></tr> <tr><td colspan="2">Byte 1</td></tr> <tr><td>0</td><td>SECLEVEL</td></tr> <tr><td>*1</td><td>NOSECLEVEL</td></tr> <tr><td>2</td><td>FROM</td></tr> <tr><td>3</td><td>FCLASS</td></tr> <tr><td>4</td><td>FVOLUME</td></tr> <tr><td>5</td><td>FGENERIC</td></tr> <tr><td>6</td><td>SECLABEL</td></tr> <tr><td>7</td><td>NOSECLABEL</td></tr> </tbody> </table>	Bit	Keyword Specified	Byte 0		0	NOTIFY	*1	NONOTIFY	2	TVTOC	*3	NOTVTOC	4	TIMEZONE	*5	NOTIMEZONE	6	ADDCATEGORY	*7	DELCATEGORY	Byte 1		0	SECLEVEL	*1	NOSECLEVEL	2	FROM	3	FCLASS	4	FVOLUME	5	FGENERIC	6	SECLABEL	7	NOSECLABEL
Bit	Keyword Specified																																									
Byte 0																																										
0	NOTIFY																																									
*1	NONOTIFY																																									
2	TVTOC																																									
*3	NOTVTOC																																									
4	TIMEZONE																																									
*5	NOTIMEZONE																																									
6	ADDCATEGORY																																									
*7	DELCATEGORY																																									
Byte 1																																										
0	SECLEVEL																																									
*1	NOSECLEVEL																																									
2	FROM																																									
3	FCLASS																																									
4	FVOLUME																																									
5	FGENERIC																																									
6	SECLABEL																																									
7	NOSECLABEL																																									
		2	Binary	Flags for keywords ignored because of insufficient authority: Same format as flags for keywords specified.																																						
		8	EBCDIC	User ID to be notified when profile denies access																																						
		44	EBCDIC	FROM resource name																																						
		6	EBCDIC	FROM volume volser																																						

Data Type 6

Event Code Dec(Hex)	Command	Data Length	Format	Description																																						
20(14) (Cont.)	RALTER (Cont.)	8	EBCDIC	FROM class name																																						
		1	Binary	LOGON days: <table border="0"> <thead> <tr> <th>Bit</th> <th>Day Specified</th> </tr> </thead> <tbody> <tr><td>0</td><td>Sunday</td></tr> <tr><td>1</td><td>Monday</td></tr> <tr><td>2</td><td>Tuesday</td></tr> <tr><td>3</td><td>Wednesday</td></tr> <tr><td>4</td><td>Thursday</td></tr> <tr><td>5</td><td>Friday</td></tr> <tr><td>6</td><td>Saturday</td></tr> <tr><td>7</td><td>No keyword</td></tr> </tbody> </table>	Bit	Day Specified	0	Sunday	1	Monday	2	Tuesday	3	Wednesday	4	Thursday	5	Friday	6	Saturday	7	No keyword																				
		Bit	Day Specified																																							
		0	Sunday																																							
		1	Monday																																							
		2	Tuesday																																							
		3	Wednesday																																							
		4	Thursday																																							
		5	Friday																																							
		6	Saturday																																							
7	No keyword																																									
3	packed	Logon time, packed. If no subkeyword, then binary zeros.																																								
3	packed	Logoff time, packed. If no subkeyword, then binary zeros.																																								
3	packed	TIMEZONE value: <table border="0"> <thead> <tr> <th>Bit</th> <th>Bit Value Specified</th> </tr> </thead> <tbody> <tr> <td colspan="2">Byte 0–2</td> </tr> <tr> <td></td> <td>Signed decimal number</td> </tr> </tbody> </table>	Bit	Bit Value Specified	Byte 0–2			Signed decimal number																																		
Bit	Bit Value Specified																																									
Byte 0–2																																										
	Signed decimal number																																									
44	EBCDIC	SECLEVEL name																																								
8	EBCDIC	SECLABEL name																																								
21(15)	RDEFINE	* The data for event code 21 is identical to the data for event code 20, with these exceptions.																																								
		2	Binary	Flags for keywords specified: <table border="0"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr> <td colspan="2">Byte 0</td> </tr> <tr><td>0</td><td>DATA</td></tr> <tr><td>1</td><td>OWNER</td></tr> <tr><td>2</td><td>UACC</td></tr> <tr><td>3</td><td>LEVEL</td></tr> <tr><td>4</td><td>AUDIT</td></tr> <tr><td>5</td><td>GLOBALAUDIT</td></tr> <tr><td>6</td><td>ADDVOL</td></tr> <tr><td>7</td><td>DELVOL</td></tr> <tr> <td colspan="2">Byte 1</td> </tr> <tr><td>0</td><td>ADDMEM</td></tr> <tr><td>1</td><td>DELMEM</td></tr> <tr><td>2</td><td>APPLDATA</td></tr> <tr><td>3</td><td>SINGLEDSN</td></tr> <tr><td>4</td><td>NOSINGLEDSN</td></tr> <tr><td>5</td><td>WARNING</td></tr> <tr><td>6</td><td>NOWARNING</td></tr> <tr><td>7</td><td>WHEN</td></tr> </tbody> </table>	Bit	Keyword Specified	Byte 0		0	DATA	1	OWNER	2	UACC	3	LEVEL	4	AUDIT	5	GLOBALAUDIT	6	ADDVOL	7	DELVOL	Byte 1		0	ADDMEM	1	DELMEM	2	APPLDATA	3	SINGLEDSN	4	NOSINGLEDSN	5	WARNING	6	NOWARNING	7	WHEN
		Bit	Keyword Specified																																							
		Byte 0																																								
		0	DATA																																							
		1	OWNER																																							
		2	UACC																																							
		3	LEVEL																																							
		4	AUDIT																																							
		5	GLOBALAUDIT																																							
6	ADDVOL																																									
7	DELVOL																																									
Byte 1																																										
0	ADDMEM																																									
1	DELMEM																																									
2	APPLDATA																																									
3	SINGLEDSN																																									
4	NOSINGLEDSN																																									
5	WARNING																																									
6	NOWARNING																																									
7	WHEN																																									
2	Binary	Flags for keywords ignored because of insufficient authority: Same format as flags for keywords specified.																																								
2	Binary	Flags for class name: <table border="0"> <thead> <tr> <th>Bit</th> <th>Option Specified</th> </tr> </thead> <tbody> <tr> <td colspan="2">Byte 0</td> </tr> <tr><td>0–3</td><td>Reserved</td></tr> <tr><td>4</td><td>DASDVOL</td></tr> <tr><td>5</td><td>TAPEVOL</td></tr> <tr><td>6</td><td>TERMINAL</td></tr> <tr><td>7</td><td>Reserved</td></tr> <tr> <td colspan="2">Byte 1</td> </tr> <tr><td>0</td><td>Generic resource name specified</td></tr> <tr><td>1–7</td><td>Reserved</td></tr> </tbody> </table>	Bit	Option Specified	Byte 0		0–3	Reserved	4	DASDVOL	5	TAPEVOL	6	TERMINAL	7	Reserved	Byte 1		0	Generic resource name specified	1–7	Reserved																				
Bit	Option Specified																																									
Byte 0																																										
0–3	Reserved																																									
4	DASDVOL																																									
5	TAPEVOL																																									
6	TERMINAL																																									
7	Reserved																																									
Byte 1																																										
0	Generic resource name specified																																									
1–7	Reserved																																									
8	EBCDIC	User ID or group name (OWNER keyword)																																								

Event Code Dec(Hex)	Command	Data Length	Format	Description																																						
21(15) (Cont.)	RDEFINE (Cont.)	1	Binary	Flags for UACC keyword: <table border="0"> <thead> <tr> <th>Bit</th> <th>Authority Specified</th> </tr> </thead> <tbody> <tr><td>0</td><td>ALTER</td></tr> <tr><td>1</td><td>CONTROL</td></tr> <tr><td>2</td><td>UPDATE</td></tr> <tr><td>3</td><td>READ</td></tr> <tr><td>4</td><td>EXECUTE</td></tr> <tr><td>5-6</td><td>Reserved</td></tr> <tr><td>7</td><td>NONE</td></tr> </tbody> </table>	Bit	Authority Specified	0	ALTER	1	CONTROL	2	UPDATE	3	READ	4	EXECUTE	5-6	Reserved	7	NONE																						
Bit	Authority Specified																																									
0	ALTER																																									
1	CONTROL																																									
2	UPDATE																																									
3	READ																																									
4	EXECUTE																																									
5-6	Reserved																																									
7	NONE																																									
		1	Binary	nn (LEVEL keyword)																																						
		1	Binary	Flags for AUDIT keyword: <table border="0"> <thead> <tr> <th>Bit</th> <th>Authority Specified</th> </tr> </thead> <tbody> <tr><td>0</td><td>ALL</td></tr> <tr><td>1</td><td>SUCCESS</td></tr> <tr><td></td><td>'00' — READ</td></tr> <tr><td></td><td>'01' — UPDATE</td></tr> <tr><td></td><td>'10' — CONTROL</td></tr> <tr><td></td><td>'11' — ALTER</td></tr> <tr><td>2</td><td>FAILURES</td></tr> <tr><td></td><td>'00' — READ</td></tr> <tr><td></td><td>'01' — UPDATE</td></tr> <tr><td></td><td>'10' — CONTROL</td></tr> <tr><td></td><td>'11' — ALTER</td></tr> <tr><td>3</td><td>NONE</td></tr> <tr><td>4-5</td><td>SUCCESS qualifier codes</td></tr> <tr><td>6-7</td><td>FAILURES qualifier codes</td></tr> </tbody> </table>	Bit	Authority Specified	0	ALL	1	SUCCESS		'00' — READ		'01' — UPDATE		'10' — CONTROL		'11' — ALTER	2	FAILURES		'00' — READ		'01' — UPDATE		'10' — CONTROL		'11' — ALTER	3	NONE	4-5	SUCCESS qualifier codes	6-7	FAILURES qualifier codes								
Bit	Authority Specified																																									
0	ALL																																									
1	SUCCESS																																									
	'00' — READ																																									
	'01' — UPDATE																																									
	'10' — CONTROL																																									
	'11' — ALTER																																									
2	FAILURES																																									
	'00' — READ																																									
	'01' — UPDATE																																									
	'10' — CONTROL																																									
	'11' — ALTER																																									
3	NONE																																									
4-5	SUCCESS qualifier codes																																									
6-7	FAILURES qualifier codes																																									
		1	Binary	*Reserved																																						
		2	Binary	Flags for keywords specified: <table border="0"> <thead> <tr> <th>Bit</th> <th>Option Specified</th> </tr> </thead> <tbody> <tr><td colspan="2">Byte 0</td></tr> <tr><td>0</td><td>NOTIFY</td></tr> <tr><td>*1</td><td>NONOTIFY</td></tr> <tr><td>2</td><td>TVTOC</td></tr> <tr><td>*3</td><td>NOTVTOC</td></tr> <tr><td>4</td><td>TIMEZONE</td></tr> <tr><td>*5</td><td>NOTIMEZONE</td></tr> <tr><td>6</td><td>ADDCATEGORY</td></tr> <tr><td>*7</td><td>DELCATEGORY</td></tr> <tr><td colspan="2">Byte 1</td></tr> <tr><td>0</td><td>SECLEVEL</td></tr> <tr><td>*1</td><td>NOSECLEVEL</td></tr> <tr><td>2</td><td>FROM</td></tr> <tr><td>3</td><td>FCLASS</td></tr> <tr><td>4</td><td>FVOLUME</td></tr> <tr><td>5</td><td>FGENERIC</td></tr> <tr><td>6</td><td>SECLABEL</td></tr> <tr><td>7</td><td>NOSECLABEL</td></tr> </tbody> </table>	Bit	Option Specified	Byte 0		0	NOTIFY	*1	NONOTIFY	2	TVTOC	*3	NOTVTOC	4	TIMEZONE	*5	NOTIMEZONE	6	ADDCATEGORY	*7	DELCATEGORY	Byte 1		0	SECLEVEL	*1	NOSECLEVEL	2	FROM	3	FCLASS	4	FVOLUME	5	FGENERIC	6	SECLABEL	7	NOSECLABEL
Bit	Option Specified																																									
Byte 0																																										
0	NOTIFY																																									
*1	NONOTIFY																																									
2	TVTOC																																									
*3	NOTVTOC																																									
4	TIMEZONE																																									
*5	NOTIMEZONE																																									
6	ADDCATEGORY																																									
*7	DELCATEGORY																																									
Byte 1																																										
0	SECLEVEL																																									
*1	NOSECLEVEL																																									
2	FROM																																									
3	FCLASS																																									
4	FVOLUME																																									
5	FGENERIC																																									
6	SECLABEL																																									
7	NOSECLABEL																																									
		2	Binary	Flags for keywords ignored because of insufficient authority. Same format as flags for keywords specified.																																						
		8	EBCDIC	User ID to be notified when profile denies access																																						
		44	EBCDIC	FROM resource name																																						

Data Type 6

Event Code Dec(Hex)	Command	Data Length	Format	Description
21(15) (Cont.)	RDEFINE (Cont.)	6	EBCDIC	FROM volume volser
		8	EBCDIC	FROM class name
		1	Binary	LOGON days:
				Bit Day Specified
				0 Sunday
				1 Monday
				2 Tuesday
				3 Wednesday
				4 Thursday
				5 Friday
				6 Saturday
		7 No keyword		
		3 packed Logon time, packed. If no subkeyword, then binary zeros.		
		3 packed Logoff time, packed. If no subkeyword, then binary zeros.		
		3 packed TIMEZONE value:		
		Bit Option Specified		
		Byte 0		
		0-7 Reserved		
		Byte 1		
		0-7 Reserved		
		Byte 2		
		0-3 Reserved		
		4-7 Time zone		
		44 EBCDIC SECLEVEL name		
		8 EBCDIC SECLABEL name		
22(16)	RDELETE	2	Binary	Flags for class name:
				Bit Option Specified
				Byte 0
				0-3 Reserved
				4 DASDVOL
				5 TAPEVOL
				6 TERMINAL
				7 Reserved
				Byte 1
				0 Generic resource name specified
				1-7 Reserved
23(17)	REMOVE	1	Binary	Flags for keywords specified:
				Bit Keyword Specified
				0 GROUP
				1 OWNER
				2-7 Reserved
				1 Binary Flags for keywords ignored because of insufficient authority: Same format as flags for keywords specified.
				8 EBCDIC User ID (to be removed)
8 EBCDIC Group name (GROUP keyword)				
8 EBCDIC User ID or group name (OWNER keyword)				

Event Code Dec(Hex)	Command	Data Length	Format	Description																																																								
24(18)	SETROPTS	3	Binary	Flags for keywords specified: <table border="1"> <thead> <tr> <th>Bit</th> <th>Option Specified</th> </tr> </thead> <tbody> <tr><td colspan="2">Byte 0</td></tr> <tr><td>0</td><td>TAPE</td></tr> <tr><td>1</td><td>NOTAPE</td></tr> <tr><td>2</td><td>INITSTATS</td></tr> <tr><td>3</td><td>NOINITSTATS</td></tr> <tr><td>4</td><td>SAUDIT</td></tr> <tr><td>5</td><td>NOSAUDIT</td></tr> <tr><td>6</td><td>STATISTICS</td></tr> <tr><td>7</td><td>NOSTATISTICS</td></tr> <tr><td colspan="2">Byte 1</td></tr> <tr><td>0</td><td>AUDIT</td></tr> <tr><td>1</td><td>NOAUDIT</td></tr> <tr><td>2</td><td>TERMINAL</td></tr> <tr><td>3</td><td>NOTERMINAL</td></tr> <tr><td>4</td><td>INTERVAL (PASSWORD)</td></tr> <tr><td>5</td><td>CMDVIOL</td></tr> <tr><td>6</td><td>NOCMDVIOL</td></tr> <tr><td>7</td><td>DASD</td></tr> <tr><td colspan="2">Byte 2</td></tr> <tr><td>0</td><td>NODASD</td></tr> <tr><td>1</td><td>CLASSACT</td></tr> <tr><td>2</td><td>NOCLASSACT</td></tr> <tr><td>3</td><td>HISTORY or NOHISTORY</td></tr> <tr><td>4</td><td>WARNING or NOWARNING</td></tr> <tr><td>5</td><td>REVOKE or NOREVOKE</td></tr> <tr><td>6</td><td>NORULES or RULEn</td></tr> <tr><td>7</td><td>INACTIVE INTERVAL</td></tr> </tbody> </table>	Bit	Option Specified	Byte 0		0	TAPE	1	NOTAPE	2	INITSTATS	3	NOINITSTATS	4	SAUDIT	5	NOSAUDIT	6	STATISTICS	7	NOSTATISTICS	Byte 1		0	AUDIT	1	NOAUDIT	2	TERMINAL	3	NOTERMINAL	4	INTERVAL (PASSWORD)	5	CMDVIOL	6	NOCMDVIOL	7	DASD	Byte 2		0	NODASD	1	CLASSACT	2	NOCLASSACT	3	HISTORY or NOHISTORY	4	WARNING or NOWARNING	5	REVOKE or NOREVOKE	6	NORULES or RULEn	7	INACTIVE INTERVAL
Bit	Option Specified																																																											
Byte 0																																																												
0	TAPE																																																											
1	NOTAPE																																																											
2	INITSTATS																																																											
3	NOINITSTATS																																																											
4	SAUDIT																																																											
5	NOSAUDIT																																																											
6	STATISTICS																																																											
7	NOSTATISTICS																																																											
Byte 1																																																												
0	AUDIT																																																											
1	NOAUDIT																																																											
2	TERMINAL																																																											
3	NOTERMINAL																																																											
4	INTERVAL (PASSWORD)																																																											
5	CMDVIOL																																																											
6	NOCMDVIOL																																																											
7	DASD																																																											
Byte 2																																																												
0	NODASD																																																											
1	CLASSACT																																																											
2	NOCLASSACT																																																											
3	HISTORY or NOHISTORY																																																											
4	WARNING or NOWARNING																																																											
5	REVOKE or NOREVOKE																																																											
6	NORULES or RULEn																																																											
7	INACTIVE INTERVAL																																																											
3			Binary	Flags for keywords ignored because of insufficient authority: Same format as flags for keywords specified.																																																								
1			Binary	Flags for STATISTICS or NOSTATISTICS keyword: <table border="1"> <thead> <tr> <th>Bit</th> <th>Option Specified</th> </tr> </thead> <tbody> <tr><td colspan="2">Byte 0</td></tr> <tr><td>0-2</td><td>Reserved</td></tr> <tr><td>3</td><td>DATASET</td></tr> <tr><td>4</td><td>DASDVOL</td></tr> <tr><td>5</td><td>TAPEVOL</td></tr> <tr><td>6</td><td>TERMINAL</td></tr> <tr><td>7</td><td>Reserved</td></tr> </tbody> </table>	Bit	Option Specified	Byte 0		0-2	Reserved	3	DATASET	4	DASDVOL	5	TAPEVOL	6	TERMINAL	7	Reserved																																								
Bit	Option Specified																																																											
Byte 0																																																												
0-2	Reserved																																																											
3	DATASET																																																											
4	DASDVOL																																																											
5	TAPEVOL																																																											
6	TERMINAL																																																											
7	Reserved																																																											
1			Binary	Flags for keywords ignored: <table border="1"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr><td>0</td><td>MODEL-GDG</td></tr> <tr><td>1</td><td>MODEL-NOGDG</td></tr> <tr><td>2</td><td>MODEL-USER</td></tr> <tr><td>3</td><td>MODEL-NOUSER</td></tr> <tr><td>4</td><td>MODEL-GROUP</td></tr> <tr><td>5</td><td>MODEL-NOGROUP</td></tr> <tr><td>6</td><td>GRPLIST</td></tr> <tr><td>7</td><td>NOGRPLIST</td></tr> </tbody> </table>	Bit	Keyword Specified	0	MODEL-GDG	1	MODEL-NOGDG	2	MODEL-USER	3	MODEL-NOUSER	4	MODEL-GROUP	5	MODEL-NOGROUP	6	GRPLIST	7	NOGRPLIST																																						
Bit	Keyword Specified																																																											
0	MODEL-GDG																																																											
1	MODEL-NOGDG																																																											
2	MODEL-USER																																																											
3	MODEL-NOUSER																																																											
4	MODEL-GROUP																																																											
5	MODEL-NOGROUP																																																											
6	GRPLIST																																																											
7	NOGRPLIST																																																											

Data Type 6

Event Code Dec(Hex)	Command	Data Length	Format	Description																
24(18) (Cont.)	SETROPTS (Cont.)	1	Binary	Flags for AUDIT or NOAUDIT keyword:																
				<table border="0"> <thead> <tr> <th>Bit</th> <th>Option Specified</th> </tr> </thead> <tbody> <tr><td>0</td><td>Reserved</td></tr> <tr><td>1</td><td>GROUP</td></tr> <tr><td>2</td><td>USER</td></tr> <tr><td>3</td><td>DATASET</td></tr> <tr><td>4</td><td>DASDVOL</td></tr> <tr><td>5</td><td>TAPEVOL</td></tr> <tr><td>6</td><td>TERMINAL</td></tr> <tr><td>7</td><td>Reserved</td></tr> </tbody> </table>	Bit	Option Specified	0	Reserved	1	GROUP	2	USER	3	DATASET	4	DASDVOL	5	TAPEVOL	6	TERMINAL
		Bit	Option Specified																	
		0	Reserved																	
		1	GROUP																	
		2	USER																	
		3	DATASET																	
		4	DASDVOL																	
		5	TAPEVOL																	
		6	TERMINAL																	
7	Reserved																			
1	Binary	Flags for keywords specified:																		
		<table border="0"> <thead> <tr> <th>Bit</th> <th>Option Specified</th> </tr> </thead> <tbody> <tr><td>0</td><td>MODEL-GDG</td></tr> <tr><td>1</td><td>MODEL-NOGDG</td></tr> <tr><td>2</td><td>MODEL-USER</td></tr> <tr><td>3</td><td>MODEL-NOUSER</td></tr> <tr><td>4</td><td>MODEL-GROUP</td></tr> <tr><td>5</td><td>MODEL-NOGROUP</td></tr> <tr><td>6</td><td>GRPLIST</td></tr> <tr><td>7</td><td>NOGRPLIST</td></tr> </tbody> </table>	Bit	Option Specified	0	MODEL-GDG	1	MODEL-NOGDG	2	MODEL-USER	3	MODEL-NOUSER	4	MODEL-GROUP	5	MODEL-NOGROUP	6	GRPLIST	7	NOGRPLIST
Bit	Option Specified																			
0	MODEL-GDG																			
1	MODEL-NOGDG																			
2	MODEL-USER																			
3	MODEL-NOUSER																			
4	MODEL-GROUP																			
5	MODEL-NOGROUP																			
6	GRPLIST																			
7	NOGRPLIST																			
1	Binary	Change-interval (INTERVAL keyword)																		
1	Binary	Flags for TERMINAL keyword:																		
		<table border="0"> <thead> <tr> <th>Bit</th> <th>Option Specified</th> </tr> </thead> <tbody> <tr><td>0-2</td><td>Reserved</td></tr> <tr><td>3</td><td>READ</td></tr> <tr><td>4-6</td><td>Reserved</td></tr> <tr><td>7</td><td>NONE</td></tr> </tbody> </table>	Bit	Option Specified	0-2	Reserved	3	READ	4-6	Reserved	7	NONE								
Bit	Option Specified																			
0-2	Reserved																			
3	READ																			
4-6	Reserved																			
7	NONE																			
1	Binary	Flags for current statistics options after SETROPTS has executed:																		
		<table border="0"> <thead> <tr> <th>Bit</th> <th>Option Specified</th> </tr> </thead> <tbody> <tr><td>0</td><td>Reserved</td></tr> <tr><td>1</td><td>Bypass RACINIT statistics</td></tr> <tr><td>2</td><td>Bypass data set statistics</td></tr> <tr><td>3</td><td>Bypass tape volume statistics</td></tr> <tr><td>4</td><td>Bypass DASD volume statistics</td></tr> <tr><td>5</td><td>Bypass terminal statistics</td></tr> <tr><td>6</td><td>Bypass ADSP attribute</td></tr> <tr><td>7</td><td>EGN in effect</td></tr> </tbody> </table>	Bit	Option Specified	0	Reserved	1	Bypass RACINIT statistics	2	Bypass data set statistics	3	Bypass tape volume statistics	4	Bypass DASD volume statistics	5	Bypass terminal statistics	6	Bypass ADSP attribute	7	EGN in effect
Bit	Option Specified																			
0	Reserved																			
1	Bypass RACINIT statistics																			
2	Bypass data set statistics																			
3	Bypass tape volume statistics																			
4	Bypass DASD volume statistics																			
5	Bypass terminal statistics																			
6	Bypass ADSP attribute																			
7	EGN in effect																			
1	Binary	Flags for current audit options after SETROPTS has executed:																		
		<table border="0"> <thead> <tr> <th>Bit</th> <th>Option Specified</th> </tr> </thead> <tbody> <tr><td>0</td><td>Reserved</td></tr> <tr><td>1</td><td>Log group class</td></tr> <tr><td>2</td><td>Log user class</td></tr> <tr><td>3</td><td>Log data set class</td></tr> <tr><td>4</td><td>Log DASD volume class</td></tr> <tr><td>5</td><td>Log tape volume class</td></tr> <tr><td>6</td><td>Log terminal class</td></tr> <tr><td>7</td><td>Reserved</td></tr> </tbody> </table>	Bit	Option Specified	0	Reserved	1	Log group class	2	Log user class	3	Log data set class	4	Log DASD volume class	5	Log tape volume class	6	Log terminal class	7	Reserved
Bit	Option Specified																			
0	Reserved																			
1	Log group class																			
2	Log user class																			
3	Log data set class																			
4	Log DASD volume class																			
5	Log tape volume class																			
6	Log terminal class																			
7	Reserved																			
1	Binary	Reserved																		

Event Code Dec(Hex)	Command	Data Length	Format	Description																																
24(18) (Cont.)	SETROPTS (Cont.)	2	Binary	Flags for miscellaneous options after SETROPTS has executed:																																
				<table border="0"> <thead> <tr> <th>Bit</th> <th>Option Specified</th> </tr> </thead> <tbody> <tr> <td colspan="2">Byte 0</td> </tr> <tr> <td>0</td> <td>Perform terminal authorization checking</td> </tr> <tr> <td>1</td> <td>Terminal UACC=NONE (if this bit is off, terminal UACC=READ)</td> </tr> <tr> <td>2</td> <td>Log RACF command violations</td> </tr> <tr> <td>3</td> <td>Log SPECIAL user activity</td> </tr> <tr> <td>5-7</td> <td>Reserved</td> </tr> <tr> <td colspan="2">Byte 1</td> </tr> <tr> <td>0</td> <td>Tape volume protection is in effect</td> </tr> <tr> <td>1</td> <td>DASD volume protection is in effect</td> </tr> <tr> <td>2</td> <td>Generic profile processing is in effect for the DATASET class</td> </tr> <tr> <td>3</td> <td>Generic command (GENCMD) processing is in effect for the DATASET class</td> </tr> <tr> <td>4</td> <td>REALDSN is in effect</td> </tr> <tr> <td>5</td> <td>JES-XBMALLRACF is in effect</td> </tr> <tr> <td>6</td> <td>JES-EARLYVERIFY is in effect</td> </tr> <tr> <td>7</td> <td>JES-BATCHALLRACF is in effect</td> </tr> </tbody> </table>	Bit	Option Specified	Byte 0		0	Perform terminal authorization checking	1	Terminal UACC=NONE (if this bit is off, terminal UACC=READ)	2	Log RACF command violations	3	Log SPECIAL user activity	5-7	Reserved	Byte 1		0	Tape volume protection is in effect	1	DASD volume protection is in effect	2	Generic profile processing is in effect for the DATASET class	3	Generic command (GENCMD) processing is in effect for the DATASET class	4	REALDSN is in effect	5	JES-XBMALLRACF is in effect	6	JES-EARLYVERIFY is in effect	7	JES-BATCHALLRACF is in effect
Bit	Option Specified																																			
Byte 0																																				
0	Perform terminal authorization checking																																			
1	Terminal UACC=NONE (if this bit is off, terminal UACC=READ)																																			
2	Log RACF command violations																																			
3	Log SPECIAL user activity																																			
5-7	Reserved																																			
Byte 1																																				
0	Tape volume protection is in effect																																			
1	DASD volume protection is in effect																																			
2	Generic profile processing is in effect for the DATASET class																																			
3	Generic command (GENCMD) processing is in effect for the DATASET class																																			
4	REALDSN is in effect																																			
5	JES-XBMALLRACF is in effect																																			
6	JES-EARLYVERIFY is in effect																																			
7	JES-BATCHALLRACF is in effect																																			
		1	Binary	Maximum password interval																																
		1	Binary	Password history generation value																																
		1	Binary	Password revoke value																																
		1	Binary	Password warning level																																
		80	Binary Binary EBCDIC	Password syntax rules (eight rules). Each rule has the following basic format: <table border="0"> <thead> <tr> <th>Byte</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Starting length value</td> </tr> <tr> <td>1</td> <td>Ending length value</td> </tr> <tr> <td>2-9</td> <td>Character content rules for each of the eight possible positions. The character values are: L = Alphanumeric A = Alphabetic N = Numeric V = Vowel C = Consonant W = No vowels</td> </tr> </tbody> </table>	Byte	Description	0	Starting length value	1	Ending length value	2-9	Character content rules for each of the eight possible positions. The character values are: L = Alphanumeric A = Alphabetic N = Numeric V = Vowel C = Consonant W = No vowels																								
Byte	Description																																			
0	Starting length value																																			
1	Ending length value																																			
2-9	Character content rules for each of the eight possible positions. The character values are: L = Alphanumeric A = Alphabetic N = Numeric V = Vowel C = Consonant W = No vowels																																			
		1	Binary	User ID inactive interval																																

Data Type 6

Event Code Dec(Hex)	Command	Data Length	Format	Description																																																								
24(18) (Cont.)	SETROPTS (Cont.)	3	Binary	Flags for keywords specified: <table border="0"> <thead> <tr> <th>Bit</th> <th>Option Specified</th> </tr> </thead> <tbody> <tr><td colspan="2">Byte 0</td></tr> <tr><td>0</td><td>ADSP</td></tr> <tr><td>1</td><td>NOADSP</td></tr> <tr><td>2</td><td>GENERIC</td></tr> <tr><td>3</td><td>NOGENERIC</td></tr> <tr><td>4</td><td>GENCMD</td></tr> <tr><td>5</td><td>NOGENCMD</td></tr> <tr><td>6</td><td>GLOBAL</td></tr> <tr><td>7</td><td>NOGLOBAL</td></tr> <tr><td colspan="2">Byte 1</td></tr> <tr><td>0</td><td>PREFIX</td></tr> <tr><td>1</td><td>NOPREFIX</td></tr> <tr><td>2</td><td>REALDSN</td></tr> <tr><td>3</td><td>NOREALDSN</td></tr> <tr><td>4</td><td>JES-XBMALLRACF</td></tr> <tr><td>5</td><td>JES-NOXBMALLRACF</td></tr> <tr><td>6</td><td>JES-BATCHALLRACF</td></tr> <tr><td>7</td><td>JES-NOBATCHALLRACF</td></tr> <tr><td colspan="2">Byte 2</td></tr> <tr><td>0</td><td>JES-EARLYVERIFY</td></tr> <tr><td>1</td><td>JES-NOEARLYVERIFY</td></tr> <tr><td>2</td><td>REFRESH</td></tr> <tr><td>3</td><td>PROTECTALL-WARNING</td></tr> <tr><td>4</td><td>PROTECTALL-FAILURE</td></tr> <tr><td>5</td><td>NOPROTECTALL</td></tr> <tr><td>6</td><td>EGN in effect</td></tr> <tr><td>7</td><td>NOEGN in effect</td></tr> </tbody> </table>	Bit	Option Specified	Byte 0		0	ADSP	1	NOADSP	2	GENERIC	3	NOGENERIC	4	GENCMD	5	NOGENCMD	6	GLOBAL	7	NOGLOBAL	Byte 1		0	PREFIX	1	NOPREFIX	2	REALDSN	3	NOREALDSN	4	JES-XBMALLRACF	5	JES-NOXBMALLRACF	6	JES-BATCHALLRACF	7	JES-NOBATCHALLRACF	Byte 2		0	JES-EARLYVERIFY	1	JES-NOEARLYVERIFY	2	REFRESH	3	PROTECTALL-WARNING	4	PROTECTALL-FAILURE	5	NOPROTECTALL	6	EGN in effect	7	NOEGN in effect
Bit	Option Specified																																																											
Byte 0																																																												
0	ADSP																																																											
1	NOADSP																																																											
2	GENERIC																																																											
3	NOGENERIC																																																											
4	GENCMD																																																											
5	NOGENCMD																																																											
6	GLOBAL																																																											
7	NOGLOBAL																																																											
Byte 1																																																												
0	PREFIX																																																											
1	NOPREFIX																																																											
2	REALDSN																																																											
3	NOREALDSN																																																											
4	JES-XBMALLRACF																																																											
5	JES-NOXBMALLRACF																																																											
6	JES-BATCHALLRACF																																																											
7	JES-NOBATCHALLRACF																																																											
Byte 2																																																												
0	JES-EARLYVERIFY																																																											
1	JES-NOEARLYVERIFY																																																											
2	REFRESH																																																											
3	PROTECTALL-WARNING																																																											
4	PROTECTALL-FAILURE																																																											
5	NOPROTECTALL																																																											
6	EGN in effect																																																											
7	NOEGN in effect																																																											
3			Binary	Flags for keywords specified but ignored because of insufficient authority: Same format as flags for keywords specified.																																																								
8			EBCDIC	Single-level data set name prefix																																																								
3			Binary	Flags for keywords specified: <table border="0"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr><td colspan="2">Byte 0</td></tr> <tr><td>0</td><td>TAPEDSN</td></tr> <tr><td>1</td><td>NOTAPEDSN</td></tr> <tr><td>2</td><td>NOEOS</td></tr> <tr><td>3</td><td>EOS</td></tr> <tr><td>4</td><td>EOS-SECLEVEL</td></tr> <tr><td>5</td><td>EOS-NOSECLEVEL</td></tr> <tr><td>6</td><td>RETPD</td></tr> <tr><td>7</td><td>WHEN</td></tr> <tr><td colspan="2">Byte 1</td></tr> <tr><td>0</td><td>NOWHEN</td></tr> <tr><td>1</td><td>OPERAUDIT</td></tr> <tr><td>2</td><td>NOOPERAUDIT</td></tr> <tr><td>3</td><td>RVARY SWITCH</td></tr> <tr><td>4</td><td>RVARY ACTIVE/INACTIVE</td></tr> <tr><td>5</td><td>ERASE-ALL</td></tr> <tr><td>6-7</td><td>Reserved</td></tr> <tr><td colspan="2">Byte 2</td></tr> <tr><td>0-7</td><td>Reserved</td></tr> </tbody> </table>	Bit	Keyword Specified	Byte 0		0	TAPEDSN	1	NOTAPEDSN	2	NOEOS	3	EOS	4	EOS-SECLEVEL	5	EOS-NOSECLEVEL	6	RETPD	7	WHEN	Byte 1		0	NOWHEN	1	OPERAUDIT	2	NOOPERAUDIT	3	RVARY SWITCH	4	RVARY ACTIVE/INACTIVE	5	ERASE-ALL	6-7	Reserved	Byte 2		0-7	Reserved																
Bit	Keyword Specified																																																											
Byte 0																																																												
0	TAPEDSN																																																											
1	NOTAPEDSN																																																											
2	NOEOS																																																											
3	EOS																																																											
4	EOS-SECLEVEL																																																											
5	EOS-NOSECLEVEL																																																											
6	RETPD																																																											
7	WHEN																																																											
Byte 1																																																												
0	NOWHEN																																																											
1	OPERAUDIT																																																											
2	NOOPERAUDIT																																																											
3	RVARY SWITCH																																																											
4	RVARY ACTIVE/INACTIVE																																																											
5	ERASE-ALL																																																											
6-7	Reserved																																																											
Byte 2																																																												
0-7	Reserved																																																											

Event Code Dec(Hex)	Command	Data Length	Format	Description
24(18) (Cont.)	SETROPTS (Cont.)	3	Binary	Flags for keywords specified but ignored because of insufficient authority: Same format as flags for keywords specified.
		1	Binary	Erase on scratch security level
		2	Binary	Retention period
		1	Binary	Flags for miscellaneous options after SETROPTS processing:
			Bit	Option Specified
			Byte 0	
			0	PROTECTALL-WARNING
			1	PROTECTALL-FAILURES
			2	EOS
			3	EOS-SECLEVEL
			4	TAPEDSN
			5	WHEN
			6	EOS ALL IN EFFECT (erase everything)
			7	Reserved
		5	Binary	Flags for keywords specified:
			Bit	Option Specified
			Byte 0	
			0-7	Reserved
			Byte 1	
			0	GENLIST
			1	NOGENLIST
			2	RACLIST
			3	NORACLIST
			4	SECLEVELAUDIT
			5	NOSECLEVELAUDIT
			6	SECLABELAUDIT
			7	NOSECLABELAUDIT
			8	SECLABELCONTROL
			9	NOSECLABELCONTROL
			10	MLQUIET
			11	NOMLQUIET
			12	MLSTABLE
			13	NOMLSTABLE
			14	GENERICOWNER
			15	NOGENERICOWNER
			16	SESSIONINTERVAL
			17	NOSESSIONINTERVAL
			18	JES NJEUSERID (userid ID)
			19	JES UNDEFINEDUSER (user ID)
			20	COMPATMODE
			21	NOCOMPATMODE
			22	MLS WARNING
			23	MLS FAILURES
			24	NOMLS
			25	MLACTIVE WARNING
			26	MLACTIVE FAILURES
			27	NOMLACTIVE
			28	CATDSNS WARNING
			29	CATDSNS FAILURES
			30	NOCATDSNS
			31	LOGOPTIONS

Data Type 6

Event Code Dec(Hex)	Command	Data Length	Format	Description	
24(18) (Cont.)	SETROPTS (Cont.)	4	Binary	Flags for keywords specified but ignored because of insufficient authority: Same format as flags for keywords specified.	
		1	Binary	SECLEVEL audit value (auditing occurs for all resources having at least this value)	
		2	Binary	SESSIONINTERVAL interval	
		1	Binary	Log options for data set	
				Bit	Keyword Specified
				0	ALWAYS
				1	NEVER
				2	SUCCESSSES
				3	FAILURES
				4	DEFAULT
				5-7	Reserved
		2	Binary		Current SETROPTS options for B1 security
				Bit	Keyword Specified
				0	SECLABELAUDIT
				1	SECLABELCONTROL
				2	MLQUIET
				3	MLSTABLE
				4	GENERICOWNER
				5	COMPATMODE
				6	MLS WARNING
				7	MLS FAILURES
				8	MLACTIVE WARNING
				9	MLACTIVE FAILURES
		10	CATDSNS WARNING		
		11	CATDSNS FAILURES		
		12	APPLAUDIT		
		13	ADDCREATOR		
		14-15	Reserved		
8	EBCDIC		User ID for JES NJEUSERID		
8	EBCDIC		User ID for JES UNDEFINEDUSER		
2	EBCDIC		Reserved		
4	Binary		Flags for keywords specified		
		Bit	Keyword Specified		
		0	Primary language specified		
		1	Secondary language specified		
		2	ADDCREATOR specified		
		3	NOADDCREATOR specified		
		4	LIST specified		
		5	KERBLVL specified		
		6	EIMREGISTRY specified		
		7	NOEIMREGISTRY specified		
4	Binary		Flags for keywords specified but ignored because of insufficient authority: same format as flags for keywords specified.		
3	EBCDIC		Primary language default		
3	EBCDIC		Secondary language default		
1	Binary		Flags for asterisk (*) specified		
		Bit	Keyword Specified		
		0	Asterisk (*) specified for GENERIC		
		1	Asterisk (*) specified for GLOBAL		
		2	Asterisk (*) specified for AUDIT		
		3	Asterisk (*) specified for STATISTICS		
		4	Asterisk (*) specified for CLASSACT		
		5	Asterisk (*) specified for GENCMD		
		6	Asterisk (*) specified for LOGOPTIONS DEFAULT		
		7	Reserved		
1	Binary		KERBLVL setting		
79	EBCDIC		Reserved		

Event Code Dec(Hex)	Command	Data Length	Format	Description																		
25(19)	RVARY	1	Binary	Flags for keywords specified:																		
				<table border="1"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>ACTIVE</td> </tr> <tr> <td>1</td> <td>INACTIVE</td> </tr> <tr> <td>2</td> <td>NOTAPE</td> </tr> <tr> <td>3</td> <td>NOCLASSACT</td> </tr> <tr> <td>4</td> <td>SWITCH</td> </tr> <tr> <td>5</td> <td>DATASET</td> </tr> <tr> <td>6</td> <td>LIST</td> </tr> <tr> <td>7</td> <td>NOLIST</td> </tr> </tbody> </table>	Bit	Keyword Specified	0	ACTIVE	1	INACTIVE	2	NOTAPE	3	NOCLASSACT	4	SWITCH	5	DATASET	6	LIST	7	NOLIST
				Bit	Keyword Specified																	
0	ACTIVE																					
1	INACTIVE																					
2	NOTAPE																					
3	NOCLASSACT																					
4	SWITCH																					
5	DATASET																					
6	LIST																					
7	NOLIST																					
Flags for other violations:																						
		1	Binary	<table border="1"> <thead> <tr> <th>Bit</th> <th>Violation</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Command denied by operator</td> </tr> <tr> <td>1</td> <td>Nonzero code returned from RACF manager during ACTIVE processing</td> </tr> <tr> <td>2-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Violation	0	Command denied by operator	1	Nonzero code returned from RACF manager during ACTIVE processing	2-7	Reserved										
Bit	Violation																					
0	Command denied by operator																					
1	Nonzero code returned from RACF manager during ACTIVE processing																					
2-7	Reserved																					
		1	Binary	Flags for other keywords specified:																		
				<table border="1"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>DATASHARE</td> </tr> <tr> <td>1</td> <td>NODATASHARE</td> </tr> </tbody> </table>	Bit	Keyword Specified	0	DATASHARE	1	NODATASHARE												
Bit	Keyword Specified																					
0	DATASHARE																					
1	NODATASHARE																					

Data Type 6

Event Code Dec(Hex)	Command	Data Length	Format	Description		
59(3B)	RACLINK	20	EBCDIC	Phase identifier (1 of 3 values: LOCAL ISSUANCE, TARGET PROCESSING, or TARGET RESPONSE)		
		2	Binary	Flags for keywords specified:		
				Bit	Option Specified	
				Byte 0		
				0	DEFINE	
				1	UNDEFINE	
				2	APPROVE	
				3-7	Reserved	
				Byte 1		
				0	PEER	
				1	MANAGED	
				2	PWSYNC	
				3	NOPWSYNC	
				4	Password supplied	
				5-7	Reserved	
				2	Binary	Reserved
				8	EBCDIC	Issuing node
		8	EBCDIC	Issuing user ID		
		8	EBCDIC	Source user ID for association (from ID keyword)		
		8	EBCDIC	Target node name		
		8	EBCDIC	Target user ID		
		8	EBCDIC	Target authorization ID (ID under whose authority the association was established)		
		4	EBCDIC	Originating system's SMF ID from where LOCAL ISSUANCE occurred		
		4	Binary	Original timestamp (local time) from when LOCAL ISSUANCE occurred		
		4	Packed	Original date when LOCAL ISSUANCE occurred Note: The preceding 3 fields contain the LOCAL ISSUANCE information for all 3 phases.		
		1	Binary	Status flags:		
			Bit	Status		
			Byte 0			
			0	Association established		
			1	Association pending		
			2	Association deleted		
			3	Password supplied is not valid		
			4	Valid password supplied		
			5	Expired password supplied		
			6	Revoked user ID		
			7	Reserved		
			Note:	When the event code qualifier is 0, and the status flags indicate no password was supplied and that the association is established, an authorization user ID was used from the association list. If the status flags indicate no password was supplied and the association is pending, no user ID in the authorization list had the appropriate authority or no association list exists.		

Event Code Dec(Hex)	Command	Data Length	Format	Description																																																																										
66(42)	RACDCERT	4	Binary	Flags for keywords specified:																																																																										
				<table border="1"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr> <td colspan="2">Byte 0</td> </tr> <tr> <td>0</td> <td>ADD</td> </tr> <tr> <td>1</td> <td>ALTER</td> </tr> <tr> <td>2</td> <td>DELETE</td> </tr> <tr> <td>3</td> <td>CONNECT</td> </tr> <tr> <td>4</td> <td>REMOVE</td> </tr> <tr> <td>5</td> <td>SITE</td> </tr> <tr> <td>6</td> <td>CERTAUTH</td> </tr> <tr> <td>7</td> <td>ICSF</td> </tr> <tr> <td colspan="2">Byte 1</td> </tr> <tr> <td>0</td> <td>TRUST</td> </tr> <tr> <td>1</td> <td>NOTRUST</td> </tr> <tr> <td>2</td> <td>ADDRING</td> </tr> <tr> <td>3</td> <td>DELRING</td> </tr> <tr> <td>4</td> <td>USAGE(PERSONAL)</td> </tr> <tr> <td>5</td> <td>USAGE(SITE)</td> </tr> <tr> <td>6</td> <td>USAGE(CERTAUTH)</td> </tr> <tr> <td>7</td> <td>DEFAULT</td> </tr> <tr> <td colspan="2">Byte 2</td> </tr> <tr> <td>0</td> <td>CONNECT(SITE)</td> </tr> <tr> <td>1</td> <td>CONNECT(CERTAUTH)</td> </tr> <tr> <td>2</td> <td>GENCERT</td> </tr> <tr> <td>3</td> <td>EXPORT</td> </tr> <tr> <td>4</td> <td>GENREQ</td> </tr> <tr> <td>5</td> <td>SIGNWITH(CERTAUTH... specified)</td> </tr> <tr> <td>6</td> <td>SIGNWITH(SITE... specified)</td> </tr> <tr> <td>7</td> <td>PASSWORD</td> </tr> <tr> <td colspan="2">Byte 3</td> </tr> <tr> <td>0</td> <td>MAP</td> </tr> <tr> <td>1</td> <td>ALTMAP</td> </tr> <tr> <td>2</td> <td>DELMAP</td> </tr> <tr> <td>3</td> <td>MULTIID</td> </tr> <tr> <td>4</td> <td>HIGHTRUST</td> </tr> <tr> <td>5</td> <td>PCICC</td> </tr> <tr> <td>6</td> <td>Reserved</td> </tr> <tr> <td>7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Keyword Specified	Byte 0		0	ADD	1	ALTER	2	DELETE	3	CONNECT	4	REMOVE	5	SITE	6	CERTAUTH	7	ICSF	Byte 1		0	TRUST	1	NOTRUST	2	ADDRING	3	DELRING	4	USAGE(PERSONAL)	5	USAGE(SITE)	6	USAGE(CERTAUTH)	7	DEFAULT	Byte 2		0	CONNECT(SITE)	1	CONNECT(CERTAUTH)	2	GENCERT	3	EXPORT	4	GENREQ	5	SIGNWITH(CERTAUTH... specified)	6	SIGNWITH(SITE... specified)	7	PASSWORD	Byte 3		0	MAP	1	ALTMAP	2	DELMAP	3	MULTIID	4	HIGHTRUST	5	PCICC	6	Reserved	7	Reserved
Bit	Keyword Specified																																																																													
Byte 0																																																																														
0	ADD																																																																													
1	ALTER																																																																													
2	DELETE																																																																													
3	CONNECT																																																																													
4	REMOVE																																																																													
5	SITE																																																																													
6	CERTAUTH																																																																													
7	ICSF																																																																													
Byte 1																																																																														
0	TRUST																																																																													
1	NOTRUST																																																																													
2	ADDRING																																																																													
3	DELRING																																																																													
4	USAGE(PERSONAL)																																																																													
5	USAGE(SITE)																																																																													
6	USAGE(CERTAUTH)																																																																													
7	DEFAULT																																																																													
Byte 2																																																																														
0	CONNECT(SITE)																																																																													
1	CONNECT(CERTAUTH)																																																																													
2	GENCERT																																																																													
3	EXPORT																																																																													
4	GENREQ																																																																													
5	SIGNWITH(CERTAUTH... specified)																																																																													
6	SIGNWITH(SITE... specified)																																																																													
7	PASSWORD																																																																													
Byte 3																																																																														
0	MAP																																																																													
1	ALTMAP																																																																													
2	DELMAP																																																																													
3	MULTIID																																																																													
4	HIGHTRUST																																																																													
5	PCICC																																																																													
6	Reserved																																																																													
7	Reserved																																																																													

|

Data Type 6

Event Code Dec(Hex)	Command	Data Length	Format	Description																				
66(42) (Cont.)	RACDCERT (Cont.)	1	Binary	Reserved																				
		8	EBCDIC	User ID (from ID keyword on RACDCERT)																				
		44	EBCDIC	Data set name																				
		32	EBCDIC	Label name																				
		8	EBCDIC	User ID (from ID sub-keyword on CONNECT, REMOVE, or GENCERT)																				
		32	EBCDIC	WITHLABEL																				
		4	Binary	SIZE																				
		10	EBCDIC	NOTBEFORE(date) in the format yyyy/mm/dd																				
		8	EBCDIC	NOTBEFORE(time) in the format hh:mm:ss																				
		10	EBCDIC	NOTAFTER(date) in the format yyyy/mm/dd																				
		8	EBCDIC	NOTAFTER(time) in the format hh:mm:ss																				
		1	Binary	FORMAT X'01' CERTB64 X'02' CERTDER X'03' PKCS12B64 X'04' PKCS12DER X'05' PKCS7B64 X'06' PKCS7DER																				
		4	Binary	More flags for keywords specified: <table border="1" style="margin-left: 20px;"> <thead> <tr> <th>Bit</th> <th>Keyword Specified</th> </tr> </thead> <tbody> <tr> <td colspan="2">Byte 0</td> </tr> <tr> <td>0</td> <td>ALTIP</td> </tr> <tr> <td>1</td> <td>ALTEMAIL</td> </tr> <tr> <td>2</td> <td>ALTDOMAIN</td> </tr> <tr> <td>3</td> <td>ALTURI</td> </tr> <tr> <td>4</td> <td>KUHANDSHAKE</td> </tr> <tr> <td>5</td> <td>KUDATAENCR</td> </tr> <tr> <td>6</td> <td>KUDOCSIGN</td> </tr> <tr> <td>7</td> <td>KUCERTSIGN</td> </tr> </tbody> </table>	Bit	Keyword Specified	Byte 0		0	ALTIP	1	ALTEMAIL	2	ALTDOMAIN	3	ALTURI	4	KUHANDSHAKE	5	KUDATAENCR	6	KUDOCSIGN	7	KUCERTSIGN
		Bit	Keyword Specified																					
Byte 0																								
0	ALTIP																							
1	ALTEMAIL																							
2	ALTDOMAIN																							
3	ALTURI																							
4	KUHANDSHAKE																							
5	KUDATAENCR																							
6	KUDOCSIGN																							
7	KUCERTSIGN																							

Record Type 81: RACF Initialization Record

RACF writes record type 81 at the completion of the initialization of RACF. This record contains:

- Record type
- Time stamp (time and date)
- Processor identification
- Name of each RACF database
- Volume identification of each RACF database
- Unit name of the RACF database
- Data set name of the UADS data set
- Volume identification of the UADS data set
- RACF options
- The maximum password interval
- The default installation language codes in effect at IPL time.

The format of record type 81 is:

Offsets

Dec.	Hex.	Name	Length	Format	Description
0	0	SMF81LEN	2	Binary	Record length.
2	2	SMF81SEG	2	Binary	Segment descriptor.

Offsets

Dec.	Hex.	Name	Length	Format	Description
4	4	SMF81FLG	1	Binary	System indicator Bit Meaning When Set 0-2 Reserved 3 MVS/SP Version 4 4 MVS/SP Version 3 5 MVS/SP Version 2 6 VS2 7 Reserved. Note: For MVS/SP Version 4, bits 3, 4, 5, and 6 will be on.
5	5	SMF81RTY	1	Binary	Record type: 81 (X'51').
6	6	SMF81TME	4	Binary	Time of day, in hundredths of a second, that the record was moved to the SMF buffer.
10	A	SMF81DTE	4	packed	Date that the record was moved to the SMF buffer, in the form 0cyydddF (where F is the sign).
14	E	SMF81SID	4	EBCDIC	System identification (from the SID parameter).
18	12	SMF81RDS	44	EBCDIC	Data set name of the RACF database for this IPL (blanks if RACF is not active).
62	3E	SMF81RVL	6	EBCDIC	Volume identification of RACF database. If the database is split among several DASD volumes, this field equals the first primary data set. If RACF is not active, this field is blank.
68	44	SMF81RUN	3	EBCDIC	Unit name of RACF database; blanks if RACF is not active. Note: If the master RACF primary database is on a device whose address is greater than X'FFF', the field will contain 'UCB' instead of the EBCDIC device name.
71	47	SMF81UDS	44	EBCDIC	Data set name of the user attribute data set (UADS) data set for this IPL.
115	73	SMF81UVL	6	EBCDIC	Volume identification of the user attribute data set (UADS) data set.
121	79	SMF81OPT	1	Binary	Options indicator Bit Meaning When Set 0 No RACROUTE REQUEST=VERIFY statistics are recorded 1 No DATASET statistics are recorded 2 RACROUTE REQUEST=VERIFY preprocessing exit routine, ICHRIX01, is active 3 RACROUTE REQUEST=AUTH preprocessing exit routine, ICHRCX01, is active 4 RACROUTE REQUEST=DEFINE preprocessing exit routine, ICHRDY01, is active 5 RACROUTE REQUEST=VERIFY post-processing exit routine, ICHRIX02, is active 6 RACROUTE REQUEST=AUTH post-processing exit routine, ICHRCX02, is active 7 New password exit routine, ICHPWX01, is active
122	7A	SMF81OP2	1	Binary	Options indicator 2 Bit Meaning When Set 0 No tape volume statistics are recorded 1 No DASD volume statistics are recorded 2 No terminal statistics are recorded 3 Command exit routine ICHCNX00 is active 4 Command exit routine ICHCCX00 is active 5 ADSP is not active 6 Encryption exit routine, ICHDEX01 is active 7 Naming convention table, ICHNCV00 is present.

SMF Records—Type 81

Offsets

Dec.	Hex.	Name	Length	Format	Description
123	7B	SMF81OP3	1	Binary	Options indicator 3 Bit Meaning When Set 0 Tape volume protection is in effect. 1 No duplicate data set names are to be defined 2 DASD volume protection is in effect 3 Record contains version indicator 4 RACROUTE REQUEST=FASTAUTH preprocessing exit routine, ICHRFX01, is active 5 RACROUTE REQUEST=LIST pre- and postprocessing exit routine, ICHRLX01, is active 6 RACROUTE REQUEST=LIST selection exit routine, ICHRLX02, is active 7 RACROUTE REQUEST=DEFINE postprocessing exit routine, ICHRDY02, is active.
124	7C	SMF81AOP	1	Binary	Audit options Bit Meaning When Set 0 User class profile changes are being logged 1 Group class profile changes are being logged 2 Data set class profile changes are being logged 3 Tape volume class profile changes are being logged 4 DASD volume class profile changes are being logged 5 Terminal class profile changes are being logged 6 RACF command violations are being logged 7 SPECIAL user activity is being logged.
125	7D	SMF81AO2	1	Binary	Audit options 2 Bit Meaning When Set 0 Operation user activity 1 Audit by security level is in effect 2-7 Reserved.
126	7E	SMF81TMO	1	Binary	Terminal verification options indicator Bit Meaning When Set 0 Terminal authorization checking is in effect 1 Universal access for undefined terminals is NONE; if not set, UACC=READ 2 REALDSN is in effect 3 JES-XBMALLRACF is in effect 4 JES-EARLYVERIFY is in effect 5 JES-BATCHALLRACF is in effect 6 RACROUTE REQUEST=FASTAUTH postprocessing exit routine, ICHRFX02, is active 7 Reserved.
127	7F	SMF81PIV	1	Binary	Maximum password interval (0-254).
128	80	SMF81REL	2	Binary	Offset to the first relocate section from the beginning of the record header.
130	82	SMF81CNT	2	Binary	Number of relocate sections.
132	84	SMF81VER	1	Binary	Version indicator (6 = RACF Version 1, Release 7). As of RACF 1.8.1, SMF81VRM is used instead.
133	85	SMF81QL	8	EBCDIC	Single-level data set name.

Offsets

Dec.	Hex.	Name	Length	Format	Description
141	8D	SMF81OP4	1	Binary	Options indicator 4 Bit Meaning When Set 0 TAPEDSN is in effect 1 PROTECT-ALL is in effect 2 PROTECT-ALL warning is in effect 3 ERASE-ON-SCRATCH is in effect 4 ERASE-ON-SCRATCH by SECLEVEL is in effect 5 ERASE-ON-SCRATCH for all data sets is in effect 6 Enhanced generic naming is in effect 7 Record contains a version, release, and modification number (see SMF81VRM).
142	8E	SMF81OP5	1	Binary	Options indicator 5 Bit Meaning When Set 0 Access control by program is in effect 1 ACEE compression/expansion exit IRRACX01 is active 2 RACROUTE REQUEST=FASTAUTH postprocessing exit ICHRFX04 is active 3 RACROUTE REQUEST=FASTAUTH preprocessing exit ICHRFX03 is active 4 SETROPTS NOADDCREATOR is active 5 IRREXV01 exit is active Note: The IRREXV01 exit point is defined to dynamic exit services. Bit 5 of SMF81OP5 indicates that an exit routine was active for this exit point at the time of the last IPL when the SMF record was written. The status can change either way multiple times throughout the life of the IPL. See the SET PROG operator command in <i>z/OS MVS System Commands</i> and the CSVDYNEX macro in <i>z/OS MVS Programming: Authorized Assembler Services Reference ALE-DYN</i> for more information. 6 ACEE compression/expansion exit IRRACX02 is active 7 Password exit routine, ICHDEX11 is active
143	8F	SMF81RPD	2	Binary	System retention period in effect.
145	91	SMF81SLV	1	Binary	Security level for ERASE-ON-SCRATCH in effect.
146	92	SMF81SLC	1	Binary	Security level for auditing in effect.
147	93	SMF81VRM	4	EBCDIC	FMID for RACF 2020 RACF 2.2 and OS/390 Security Server (RACF) V1 R2 2030 OS/390 Security Server (RACF) V1 R3 2040 OS/390 Security Server (RACF) V2 R4 2060 OS/390 Security Server (RACF) V2 R6 2608 OS/390 Security Server (RACF) V2 R8 7703 OS/390 Security Server (RACF) V2 R10 and z/OS Security Server (RACF) V1 R1 7705 z/OS Security Server (RACF) V1 R2
151	97	SMF81BOP	1	Binary	SETROPTS options. Bit Meaning When Set 0 SECLABELCONTROL is in effect 1 CATDSNS is in effect 2 MLQUIET is in effect 3 MLSTABLE is in effect 4 MLS is in effect 5 MLACTIVE is in effect 6 GENERICOWNER is in effect 7 SECLABELAUDIT is in effect.
152	98	SMF81SIN	2	Binary	Partner LU-verification session key interval.

SMF Records—Type 81

Offsets

Dec.	Hex.	Name	Length	Format	Description
154	9A	SMF81JSY	8	EBCDIC	JES NJE NAME user ID.
162	A2	SMF81JUN	8	EBCDIC	JES UNDEFINEDUSER user ID.
170	AA	SMF81BOX	1	Binary	SETROPTS option extensions.
				Bit	Meaning When Set
				0	COMPATMODE is in effect
				1	CATDSNS failures are in effect
				2	MLS failures are in effect
				3	MLACTIVE failures are in effect
				4	APPLAUDIT in effect
				5	Zero (0) equals default RVAR Y SWITCH password in effect. One (1) equals installation-defined RVAR Y SWITCH password in effect.
				6	Zero (0) equals default RVAR Y STATUS password in effect. One (1) equals installation-defined RVAR Y STATUS password in effect.
				7	Reserved.
171	AB	SMF81PRI	3	EBCDIC	Default primary language for an installation.
172	AC	SMF81SEC	3	EBCDIC	Default secondary language for an installation.
177	B1	SMF81KBL	1	Binary	Level of KERB segment processing in effect.
178	B2		77		Reserved.
Relocate Section:					
0	0	SMF81DTP	1	Binary	Data type.
1	1	SMF81DLN	1	Binary	Length of data that follows.
2	2	SMF81DTA	1-255	mixed	Data.

Record Type 83: RACF Processing Record for Auditing Data Sets

Record type 83 subtype 1 is a RACF processing record for auditing data sets that are affected by a RACF command (ADDSD, ALTDSD, and DELDSD) that caused the SECLABEL to be changed.

Notes:

- SMF type 83 subtype 1 records are generated when SETROPTS MLACTIVE is in effect and a RACF command (ALTDSD, ADDSD, DELDSD) has been issued that changed the security label of a data set profile. The SMF type 83 subtype 1 record contains the names of the cataloged data sets affected by the security label change.

A link value is contained in both the SMF type 80 record for the RACF command and the SMF type 83 subtype 1 record. The link value is used to connect the list of data set names affected by the security label change with the RACF command that caused the change.

- The event codes and qualifiers for type 83 records are the same as for type 80 records.

The format is:

Offsets

Dec.	Hex.	Name	Length	Format	Description
0	0	SMF83LEN	2	Binary	Record length.
2	2	SMF83SEG	2	Binary	Segment descriptor.

Offsets

Dec.	Hex.	Name	Length	Format	Description
4	4	SMF83FLG	1	Binary	System indicator Bit Meaning When Set 0 Subsystem identification follows system identification 1 Subtypes used 2 Reserved 3 MVS/SP Version 4 4 MVS/SP Version 3 5 MVS/SP Version 2 6 VS2 7 Reserved. Note: For MVS/SP Version 4, bits 3, 4, 5, and 6 will be on.
5	5	SMF83RTY	1	Binary	Record type: 83 (X'53').
6	6	SMF83TME	4	Binary	Time of day, in hundredths of a second, that the record was moved to the SMF buffer.
10	A	SMF83DTE	4	EBCDIC	Date that the record was moved to the SMF buffer, in the form <i>OcyyddF</i> (where <i>F</i> is the sign).
14	E	SMF83SID	4	EBCDIC	System identification (from the SID parameter).
18	12	SMF83SSI	4	EBCDIC	Subsystem identification — RACF.
22	16	SMF83TYP	2	Binary	Record subtype=1.
24	18	SMF83TRP	2	Binary	Number of triplets.
26	1A	SMF83XXX	2		Reserved.
28	1C	SMF83OPD	4	Binary	Offset to product section.
32	20	SMF83LPD	2	Binary	Length of product section.
34	22	SMF83NPD	2	Binary	Number of product sections.
36	24	SMF83OD1	4	Binary	Offset to security section.
40	28	SMF83LD1	2	Binary	Length of security section.
42	2A	SMF83ND1	2	Binary	Number of security sections.
44	2C	SMF83OD2	4	Binary	Offset to relocate section.
48	30	SMF83LD2	2	Binary	Length of relocate section.
50	32	SMF83ND2	2	Binary	Number of relocate sections.
Product Section:					
0	0	SMF83RVN	4	EBCDIC	RACF version, release, and modification level number.
4	4	SMF83PNM	4	EBCDIC	Product name — RACF.

Subtype 1

Offsets

Dec.	Hex.	Name	Length	Format	Description
Security Section:					
0	0	SMF83LNK	4	Binary	Same LINK value as that in the SMF type 80 record for the associated command. Connects the data set names in type 83 records with the RACF command that caused the SECLABEL change.

SMF Records—Type 83

Offsets

Dec.	Hex.	Name	Length	Format	Description
4	4	SMF83DES	2	Binary	Descriptor flags Bit Meaning When Set 0 The event is a violation 1 User is not defined to RACF 2 Record contains a version indicator (see SMF83VER) 3 The event is a warning 4 Record contains a version, release, and modification level number (see SMF83VRM) 5-15 Reserved.
6	6	SMF83EVT	1	Binary	Event code.
7	7	SMF83EVQ	1	Binary	Event code qualifier.
8	8	SMF83USR	8	EBCDIC	Identifier of the user associated with this event (jobname is used if the user is not defined to RACF).
16	10	SMF83GRP	8	EBCDIC	Group to which the user was connected (stepname is used if the user is not defined to RACF).
24	18	SMF83REL	2	Binary	Offset to the first relocate section from beginning of record header.
26	1A	SMF83CNT	2	Binary	Count of the number of relocate sections.
28	1C	SMF83ATH	1	Binary	Authorities used for executing commands or accessing resources Bit Meaning When Set 0 Normal authority check (resource access) 1 SPECIAL attribute (command processing) 2 OPERATIONS attribute (resource access, command processing) 3 AUDITOR attribute (command processing) 4 Installation exit processing (resource access) 5 Failsoft processing (resource access) 6 Bypassed-user ID = *BYPASS* (resource access) 7 Trusted attribute (resource access).
29	1D	SMF83REA	1	Binary	Reason for logging. These flags indicate the reason RACF produced the SMF record Bit Meaning When Set 0 SETROPTS AUDIT(class) — changes to this class of profile are being audited. 1 User being audited 2 SPECIAL users being audited 3 Access to the resource is being audited due to the AUDIT option (specified when profile created or altered by a RACF command), a logging request from the RACHECK exit routine, or because the operator granted access during failsoft processing. 4 RACINIT failure 5 This command is always audited 6 Violation detected in command and CMDVIOL is in effect 7 Access to entity being audited due to GLOBALAUDIT option.
30	1E	SMF83TLV	1	Binary	Terminal level number of foreground user (zero if not available).

Offsets

Dec.	Hex.	Name	Length	Format	Description
31	1F	SMF83ERR	1	Binary	Command processing error flag Bit Meaning When Set 0 Command had error and RACF could not back out some changes 1 No profile updates were made because of error in RACF processing 2-7 Reserved.
32	20	SMF83TRM	8	EBCDIC	Terminal ID of foreground user (zero if not available).
40	28	SMF83JBN	8	EBCDIC	Job name. For RACROUTE REQUEST=VERIFY and RACROUTE REQUEST=VERIFYX records for batch jobs, this field can be zero.
48	30	SMF83RST	4	Binary	Time, in hundredths of a second that the reader recognized the JOB statement for this job for RACROUTE REQUEST=VERIFY and RACROUTE REQUEST=VERIFYX records for batch jobs, this field can be zero.
52	34	SMF83RSD	4	packed	Date the reader recognized the JOB statement for this job in the form 0cyydddF (where F is the sign) for RACROUTE REQUEST=VERIFY and RACROUTE REQUEST=VERIFYX records for batch jobs, this field can be zero.
56	38	SMF83UID	8	EBCDIC	User identification field from the SMF common exit parameter area. For RACROUTE REQUEST=VERIFY and RACROUTE REQUEST=VERIFYX records for batch jobs, this field can be zero.
64	40	SMF83VER	1	Binary	Version indicator 8 = Version 1, Release 8 or later. As of RACF 1.8.1, SMF83VRM is used instead.
65	41	SMF83RE2	1	Binary	Additional reasons for logging Bit Meaning When Set 0 Security level control for auditing 1 Auditing by LOGOPTIONS 2 Class being audited due to SETROPTS SECLABELAUDIT 3 Class being audited due to SETROPTS COMPATMODE 4-7 Reserved.
66	42	SMF83VRM	4	EBCDIC	FMID for RACF 2020 RACF 2.2 and OS/390 Security Server (RACF) V1 R2 2030 OS/390 Security Server (RACF) V1 R3 2040 OS/390 Security Server (RACF) V2 R4 2060 OS/390 Security Server (RACF) V2 R6 2608 OS/390 Security Server (RACF) V2 R8 7703 OS/390 Security Server (RACF) V2 R10 and z/OS Security Server (RACF) V1 R1 7705 z/OS Security Server (RACF) V1 R2
70	46	SMF83SEC	8	EBCDIC	Security label of the user.
Relocate Section:					
0	0	SMF83DTP	1	Binary	Data type
1	1	SMF83DLN	1	Binary	Length of data that follows.
2	2	SMF83DTA	1-255	mixed	Data. Possible relocate section elements are data types 62 and 63. See Table 2, (Relocate Section Variable Data,) in the SMF Type 80 records.

Reformatted RACF SMF Records

For sorting purposes, the RACF report writer reformats SMF records (types 20, 30, 80, 81 and 83) and uses these reformatted records as input to the modules that produce the RACF reports. If you want to use the RACF report writer exit routine (ICHRSMFE) to produce additional reports or to add additional record selection criteria, you should familiarize yourself with the layouts of these reformatted records.

Record type 20 (job initiation) is written at job initiation (including TSO and VM logon). Record type 30 (common address space work record) is written at normal or abnormal termination of a batch job or step, a TSO session, or a started task. Record type 30 is also written at the expiration of an accounting interval if INTERVAL is specified in SMFPRMxx, at the start of a job (or at the start of the first step after a warm start), and at the expiration of an accounting interval for a system address space. Record types 20 and 30 are documented in *z/OS MVS System Management Facilities (SMF)*.

There are two record types—reformatted process records and reformatted status records.

Prior to RACF Release 1.7, record types 80 and 81 have had a different mapping in each release. This meant that you had to change the exit routines with each RACF release, and that the routines had to accommodate records with different mappings. Starting with Release 1.7, RACF restructured these records so that:

- All records have a common format, independent of which release created them.
- Future changes to the records can be made without requiring changes to the exit routines (unless you want to process fields that may be added in future releases).

Notes:

1. The layouts of reformatted process and status records are the same up to the record dependent sections.

Reformatted Process Records

RACF SMF record types 20, 30, 80 and 83 become reformatted process records. These records are variable in length. Note that a RACF SMF record type 80 generated by a SETROPTS or an RVARY command also causes the creation of a reformatted status record.

The layout of the common section of the reformatted process record is:

Offsets

Dec.	Hex.	Name	Length	Format	Description
0	0	RCDLEN	2	binary	Total record length
2	2	-	2	binary	Reserved
4	4	RCDRELNO	1	binary	Release of RACF
5	5	RCDREFMT	1	binary	Reformat indicator (if this byte is X'00', the record has been reformatted to the RACF Version 1 Release 6/7 format)
6	6	RCDSYSID	4	EBCDIC	System identification
10	A	RCDTYPE	1	EBCDIC	Record type (80 decimal)
11	B	RCDTIME	4	packed	Unsigned packed decimal in the form HHMMSSSTH
15	F		1	EBCDIC	Reserved

Reformatted SMF Records

Offsets

Dec.	Hex.	Name	Length	Format	Description												
16	10	RCDDATE	3	packed	Date in form YYDDDF, where F is the sign												
19	13	RCDFIXLN	2	binary	Offset from the start of the record to the first relocate section												
21	15	RCDCOMLN	2	binary	Offset from the start of the record to the record dependent fields												
23	17	RCDCNT	2	binary	Number of relocate segments												
25	19	RCDEVENT	1	binary	Event code												
26	1A	RCDQUAL	1	binary	Event code qualifier												
27	1B	RCD80FLG	1	binary	Descriptor flags: <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>This record is for security violations.</td> </tr> <tr> <td>1</td> <td>This record is for a job/step, not a user/group.</td> </tr> <tr> <td>2</td> <td>This record is truncated.</td> </tr> <tr> <td>3</td> <td>This record is for a warning.</td> </tr> <tr> <td>4-7</td> <td>Reserved.</td> </tr> </tbody> </table>	Bit	Meaning When Set	0	This record is for security violations.	1	This record is for a job/step, not a user/group.	2	This record is truncated.	3	This record is for a warning.	4-7	Reserved.
Bit	Meaning When Set																
0	This record is for security violations.																
1	This record is for a job/step, not a user/group.																
2	This record is truncated.																
3	This record is for a warning.																
4-7	Reserved.																
28	1C		1	binary	Reserved												
29	1D	RCDUSER	8	EBCDIC	Identifier of the user for which this event is recorded (or jobname if the user is not defined to RACF)												
37	25	RCDGROUP	8	EBCDIC	Group to which the user was connected (or stepname if the user is not defined to RACF)												
45	2D	RCDLOGCL	1	binary	Type of event by number: <table border="0"> <thead> <tr> <th>Number</th> <th>Type</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>LOGON/ JOB</td> </tr> <tr> <td>2</td> <td>Entity access</td> </tr> <tr> <td>3</td> <td>RACF command</td> </tr> </tbody> </table>	Number	Type	1	LOGON/ JOB	2	Entity access	3	RACF command				
Number	Type																
1	LOGON/ JOB																
2	Entity access																
3	RACF command																
46	2E	RCDCLASS	8	EBCDIC	Resource class name (see Note 1). This field contains binary zeros for records written by the RVARY and SETROPTS commands.												
54	36	RCDNAME	44	EBCDIC	Resource name (see Notes 1 and 6). This field contains the user ID for a LOGON/JOB; the resource name for a resource access.												
98	62	RCDJOBID	8	EBCDIC	Job name												
106	6A		1	EBCDIC	Reserved												
107	6B	RCDDATID	3	packed	Date that the reader recognized the JOB card for this job in the form YYDDDF												
110	6E	RCDTIMID	4	EBCDIC	Time that the reader recognized the JOB card for this job in the form HHMMSSSTH												
114	72	RCDUSRDA	8	EBCDIC	User identification field												
122	7A	RCD80TRM	8	EBCDIC	Terminal identification field												
130	82	RCD80TML	1	binary	Terminal level number												
131	83	RCDOWNER	8	EBCDIC	Owner of the resource												
139	8B	RCDUSRSM	20	EBCDIC	User name												
159	9F	RCDVRM	4	EBCDIC	Release, version and modification number												
163	A3	RCDSEC	8	EBCDIC	User's SECLABEL												
171	AB	RCDLINK	4	binary	LINK to connect data sets affected by a SECLABEL change with RACF command (ALTDSD, ADDSD, DELDSD) that caused the change.												
175	AF	RCDSTYPE	2	binary	SMF record subtype												
177	B1	RCDNAMEO	2	binary	See Note 6. Offset in variable section to relocate section type if entity name is greater than 44 characters or 'X'7FFF' if resource name is less than or equal to 44 characters.												
179	B3	RCDPVAU1	4	binary	The APPLAUDIT key, part 1 of 2												

Reformatted SMF Records

Offsets

Dec.	Hex.	Name	Length	Format	Description
183	B7	RCDPVAU2	4	binary	The APPLAUDIT key, part 2 of 2

For process records, the record-dependent section is:

Offsets

Dec.	Hex.	Name	Length	Format	Description																						
0	0	RCD80ATH	1	binary	Authority used: <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr><td>0</td><td>Normal authority</td></tr> <tr><td>1</td><td>SPECIAL attribute</td></tr> <tr><td>2</td><td>OPERATIONS attribute</td></tr> <tr><td>3</td><td>AUDITOR attribute</td></tr> <tr><td>4</td><td>Exit routine granted authority</td></tr> <tr><td>5</td><td>Failsoft processing</td></tr> <tr><td>6</td><td>Bypassed-user ID="BYPASS"</td></tr> <tr><td>7</td><td>Trusted attribute</td></tr> </tbody> </table>	Bit	Meaning When Set	0	Normal authority	1	SPECIAL attribute	2	OPERATIONS attribute	3	AUDITOR attribute	4	Exit routine granted authority	5	Failsoft processing	6	Bypassed-user ID="BYPASS"	7	Trusted attribute				
Bit	Meaning When Set																										
0	Normal authority																										
1	SPECIAL attribute																										
2	OPERATIONS attribute																										
3	AUDITOR attribute																										
4	Exit routine granted authority																										
5	Failsoft processing																										
6	Bypassed-user ID="BYPASS"																										
7	Trusted attribute																										
1	1	RCD80REA	2	binary	Reason for logging: <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr><td>0</td><td>Class being audited</td></tr> <tr><td>1</td><td>User being audited</td></tr> <tr><td>2</td><td>Special user being audited</td></tr> <tr><td>3</td><td>Resource being audited, installation-requested logging in effect, or failsoft processing</td></tr> <tr><td>4</td><td>RACINIT failures being audited</td></tr> <tr><td>5</td><td>Command always causes auditing</td></tr> <tr><td>6</td><td>Command violations being audited</td></tr> <tr><td>7</td><td>Audited because GLOBALAUDIT option in effect</td></tr> <tr><td>8</td><td>SECLEVEL audit</td></tr> <tr><td>9-15</td><td>Contains the remaining data from SMF80RE2</td></tr> </tbody> </table>	Bit	Meaning When Set	0	Class being audited	1	User being audited	2	Special user being audited	3	Resource being audited, installation-requested logging in effect, or failsoft processing	4	RACINIT failures being audited	5	Command always causes auditing	6	Command violations being audited	7	Audited because GLOBALAUDIT option in effect	8	SECLEVEL audit	9-15	Contains the remaining data from SMF80RE2
Bit	Meaning When Set																										
0	Class being audited																										
1	User being audited																										
2	Special user being audited																										
3	Resource being audited, installation-requested logging in effect, or failsoft processing																										
4	RACINIT failures being audited																										
5	Command always causes auditing																										
6	Command violations being audited																										
7	Audited because GLOBALAUDIT option in effect																										
8	SECLEVEL audit																										
9-15	Contains the remaining data from SMF80RE2																										
3	3	RCD80ERR	1	binary	Error indicators: <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr><td>0</td><td>Command could not recover</td></tr> <tr><td>1</td><td>Profile not altered</td></tr> <tr><td>2-7</td><td>Reserved</td></tr> </tbody> </table>	Bit	Meaning When Set	0	Command could not recover	1	Profile not altered	2-7	Reserved														
Bit	Meaning When Set																										
0	Command could not recover																										
1	Profile not altered																										
2-7	Reserved																										
4	4	RCDQUAL1	8	EBCDIC	Qualifier for old data set name (see Note 2)																						
12	C	RCDQUAL2	8	EBCDIC	Qualifier for new data set name (see Note 3)																						
20	14	RCDDLEV	1	binary	Data set level number (see Note 4)																						
21	15	RCDDINT	1	binary	Access authority requested: (see Note 4) <table border="0"> <thead> <tr> <th>Bit</th> <th>Access Authority</th> </tr> </thead> <tbody> <tr><td>0</td><td>ALTER</td></tr> <tr><td>1</td><td>CONTROL</td></tr> <tr><td>2</td><td>UPDATE</td></tr> <tr><td>3</td><td>READ</td></tr> <tr><td>4-7</td><td>Reserved.</td></tr> </tbody> </table>	Bit	Access Authority	0	ALTER	1	CONTROL	2	UPDATE	3	READ	4-7	Reserved.										
Bit	Access Authority																										
0	ALTER																										
1	CONTROL																										
2	UPDATE																										
3	READ																										
4-7	Reserved.																										
22	16	RCDDALWD	1	binary	Access authority allowed: (see Note 4) <table border="0"> <thead> <tr> <th>Bit</th> <th>Access Authority</th> </tr> </thead> <tbody> <tr><td>0</td><td>ALTER</td></tr> <tr><td>1</td><td>CONTROL</td></tr> <tr><td>2</td><td>UPDATE</td></tr> <tr><td>3</td><td>READ</td></tr> <tr><td>4</td><td>NONE</td></tr> <tr><td>5</td><td>EXECUTE</td></tr> <tr><td>6-7</td><td>Reserved</td></tr> </tbody> </table>	Bit	Access Authority	0	ALTER	1	CONTROL	2	UPDATE	3	READ	4	NONE	5	EXECUTE	6-7	Reserved						
Bit	Access Authority																										
0	ALTER																										
1	CONTROL																										
2	UPDATE																										
3	READ																										
4	NONE																										
5	EXECUTE																										
6-7	Reserved																										
23	17	RCDDVOL	6	EBCDIC	Volume serial (see Note 4)																						
29	1D	RCDDOLDV	6	EBCDIC	OLDVOL volume serial (see Note 4)																						

Offsets

Dec.	Hex.	Name	Length	Format	Description
35	23	RCD80GNS	1	binary	1=Generic name specified
36	24	RCD80GSP	1	binary	1=Generic name specified on FROM keyword of PERMIT
37	25	RCD80RRF	1	binary	1=The old name of the RACROUTE REQUEST=DEFINE-renamed data set from data type 33 relocate section
38	26	RCD80RRT	1	binary	1=The new name of the RACROUTE REQUEST=DEFINE-renamed data set from data type 33 relocate section
39	27	RCDGENAM	44	EBCDIC	Generic profile used or generic resource name (see Note 7)
83	53	RCDGNNMF	44	EBCDIC	Generic profile used on RACROUTE REQUEST=DEFINE RENAME or generic resource name on RACROUTE REQUEST=DEFINE RENAME Relocate Section: (See Notes 5 and 8)
127	7F	RCDGENAO	2	binary	See Note 7
129	81	RCDGNMNO	2	binary	See Note 8

Variable Relocate Section Map

+0	+0	RCDDTYPE	1	binary	Data type
+1	+1	RCDDLGT	1	binary	Length of data that follows
+2	+2	RCDDATA	variable	mixed	Data

Note 1: In order to support sorting by resource class name and resource name for the list report, the RACF report writer ensures that these fields contain valid names. The following table indicates the resource class names and the resource names assigned by the RACF report writer for each of the event codes in RCDEVENT. (Uppercase letters indicate that the value appears as shown, lowercase letters identify the field in the SMF type 80 record from which the name is obtained, and a number in parentheses identifies the relocate section in the SMF type 80 record from which the name is obtained.)

If RCDEVENT Is	Resource Class Name	Resource Name
1	USER	user ID (SMF80USR)
2	class name (17)	resource name (1)
3	class name (17)	resource name (1)
4	class name (17)	resource name (1)
5	class name (17)	resource name (1)
6	class name (17)	resource name (1)
7	class name (17)	resource name (1)
8	DATASET	data set name (6)
9	GROUP	group name (6)
10	USER	user ID (6)
11	DATASET	data set name (6)
12	GROUP	group name (6)
13	USER	user ID (6)
14	USER	user ID (6)
15	DATASET	data set name (6)
16	GROUP	group name (6)
17	USER	user ID (6)

Reformatted SMF Records

If RCDEVENT Is	Resource Class Name	Resource Name
18	USER	user ID (6)
19	class name (17)	resource name (9)
20	class name (17)	resource name (9)
21	class name (17)	resource name (9)
22	class name (17)	resource name (9)
23	USER	user ID (6)
24	none	none
25	none	none

Note 2: The RACF report writer compares this field to the DSQUAL keyword specified on the EVENT subcommand. The report writer initializes RCDQUAL1 to the high-level qualifier of the old data set name found in RCDNAME at offset 41 (29 hex) of this record. The RACF report writer exit routine, ICHRSMFE, can modify this field.

Note 3: The RACF report writer compares this field to the NEWDSQUAL keyword specified on the EVENT subcommand. The report writer initializes RCDQUAL to the high-level qualifier of the new data set name found in the relocate section for data type 2 (SMF80DTP = 2). The RACF report writer exit routine, ICHRSMFE, can modify this field.

Note 4: This field is present for event codes 2–7 (SMF80EVT=2 through SMF80EVT=7) only.

Note 5: See “Table of Event Codes and Event Code Qualifiers” on page 42 and “Table of Relocate Section Variable Data” on page 54 earlier in this chapter for a further explanation of these event codes and data types.

Note 6: With RACF 1.9 or later, entity names can be a maximum of 254 characters. Entity names containing 45–254 characters are referred to as *long* names. Field RCDNAME cannot be expanded in order to support existing reformatted records. Long resource names are handled as follows:

Field RCDNAMEO will contain the offset in the variable section of the reformatted record of relocate type which contains the long resource name.
Field RCDNAMEO will be X'7FFF' if the resource name is less than or equal to 44 characters in length.

Note 7: With RACF 1.9 or later, entity names can be a maximum of 254 characters. Field RCDGENAM cannot be expanded in order to support existing reformatted records. Long resource names are handled as follows:

Field RCDGENAO will contain the offset in the variable section of the reformatted record of relocate type which contains the long resource name.
Field RCDGENAO will be X'7FFF' if the resource name is less than or equal to 44 characters in length.

Note 8: With RACF 1.9 or later, entity names can be a maximum of 254 characters. Field RCDGNNMF cannot be expanded in order to support existing reformatted records. Long resource names are handled as follows:

Field RCDGNNMO will contain the offset in the variable section of the reformatted record of relocate type which contains the long resource name.

Field RCDGNNMO will be X'7FFF' if the resource name is less than or equal to 44 characters in length.

Reformatted Status Records

RACF SMF record types 80 (only those generated by the SETROPTS or RVARY command) and 81 become reformatted status records.

Notes:

1. The layouts of reformatted status and process records are the same up to the record dependent sections.

For status records, the record-dependent section is:

Offsets

Dec.	Hex.	Name	Length	Format	Description																		
0	00	RCDRACFD	44	EBCDIC	Name of the RACF database for this IPL																		
44	2C	RCDRACFV	6	EBCDIC	Volume identification of RACF database																		
50	32	RCDRACFU	3	EBCDIC	Unit name of RACF database																		
53	35	RCD81FLG	1	binary	Options indicators: <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>No RACROUTE REQUEST=VERIFY statistics are recorded</td> </tr> <tr> <td>1</td> <td>No DATASET statistics are recorded</td> </tr> <tr> <td>2</td> <td>RACROUTE REQUEST=VERIFY preprocessing exit routine, ICHRIX01, is active</td> </tr> <tr> <td>3</td> <td>RACROUTE REQUEST=AUTH preprocessing exit routine, ICHRCX01, is active</td> </tr> <tr> <td>4</td> <td>RACROUTE REQUEST=DEFINE preprocessing exit routine, ICHRDY01, is active</td> </tr> <tr> <td>5</td> <td>RACROUTE REQUEST=VERIFY postprocessing exit routine, ICHRIX02, is active</td> </tr> <tr> <td>6</td> <td>RACROUTE REQUEST=AUTH postprocessing exit routine, ICHRCX02, is active</td> </tr> <tr> <td>7</td> <td>New password exit routine, ICHPWX01, is active</td> </tr> </tbody> </table>	Bit	Meaning When Set	0	No RACROUTE REQUEST=VERIFY statistics are recorded	1	No DATASET statistics are recorded	2	RACROUTE REQUEST=VERIFY preprocessing exit routine, ICHRIX01, is active	3	RACROUTE REQUEST=AUTH preprocessing exit routine, ICHRCX01, is active	4	RACROUTE REQUEST=DEFINE preprocessing exit routine, ICHRDY01, is active	5	RACROUTE REQUEST=VERIFY postprocessing exit routine, ICHRIX02, is active	6	RACROUTE REQUEST=AUTH postprocessing exit routine, ICHRCX02, is active	7	New password exit routine, ICHPWX01, is active
Bit	Meaning When Set																						
0	No RACROUTE REQUEST=VERIFY statistics are recorded																						
1	No DATASET statistics are recorded																						
2	RACROUTE REQUEST=VERIFY preprocessing exit routine, ICHRIX01, is active																						
3	RACROUTE REQUEST=AUTH preprocessing exit routine, ICHRCX01, is active																						
4	RACROUTE REQUEST=DEFINE preprocessing exit routine, ICHRDY01, is active																						
5	RACROUTE REQUEST=VERIFY postprocessing exit routine, ICHRIX02, is active																						
6	RACROUTE REQUEST=AUTH postprocessing exit routine, ICHRCX02, is active																						
7	New password exit routine, ICHPWX01, is active																						
54	36	RCDUVOL	6	EBCDIC	Volume identification of UADS data set																		
60	3C	RCDUDSN	44	EBCDIC	Data set name of the UADS data set for this IPL																		
104	68	RCD81FG2	1	binary	Options indicators: <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>No tape volume statistics are recorded</td> </tr> <tr> <td>1</td> <td>No DASD volume statistics are recorded</td> </tr> <tr> <td>2</td> <td>No terminal statistics are recorded</td> </tr> <tr> <td>3</td> <td>Command exit routine ICHCNX00 is active</td> </tr> <tr> <td>4</td> <td>Command exit routine ICHCCX00 is active</td> </tr> <tr> <td>5</td> <td>ADSP is not active</td> </tr> <tr> <td>6</td> <td>Encryption exit routine, ICHDEX01, is active</td> </tr> <tr> <td>7</td> <td>Naming convention table, ICHNCV00, is present</td> </tr> </tbody> </table>	Bit	Meaning When Set	0	No tape volume statistics are recorded	1	No DASD volume statistics are recorded	2	No terminal statistics are recorded	3	Command exit routine ICHCNX00 is active	4	Command exit routine ICHCCX00 is active	5	ADSP is not active	6	Encryption exit routine, ICHDEX01, is active	7	Naming convention table, ICHNCV00, is present
Bit	Meaning When Set																						
0	No tape volume statistics are recorded																						
1	No DASD volume statistics are recorded																						
2	No terminal statistics are recorded																						
3	Command exit routine ICHCNX00 is active																						
4	Command exit routine ICHCCX00 is active																						
5	ADSP is not active																						
6	Encryption exit routine, ICHDEX01, is active																						
7	Naming convention table, ICHNCV00, is present																						

Reformatted SMF Records

Offsets

Dec.	Hex.	Name	Length	Format	Description																		
105	69	RCD81OP3	1	binary	Options indicators: <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Tape volume protection in effect</td> </tr> <tr> <td>1</td> <td>No duplicate data set protection in effect</td> </tr> <tr> <td>2</td> <td>DASD volume protection in effect</td> </tr> <tr> <td>3</td> <td>Reserved</td> </tr> <tr> <td>4</td> <td>RACROUTE REQUEST=FASTAUTH preprocessing exit routine (ICHRFX01) is active</td> </tr> <tr> <td>5</td> <td>RACROUTE REQUEST=LIST pre- and postprocessing exit routine is active</td> </tr> <tr> <td>6</td> <td>RACROUTE REQUEST=LIST selection exit routine is active</td> </tr> <tr> <td>7</td> <td>RACROUTE REQUEST=DEFINE postprocessing exit routine is active</td> </tr> </tbody> </table>	Bit	Meaning When Set	0	Tape volume protection in effect	1	No duplicate data set protection in effect	2	DASD volume protection in effect	3	Reserved	4	RACROUTE REQUEST=FASTAUTH preprocessing exit routine (ICHRFX01) is active	5	RACROUTE REQUEST=LIST pre- and postprocessing exit routine is active	6	RACROUTE REQUEST=LIST selection exit routine is active	7	RACROUTE REQUEST=DEFINE postprocessing exit routine is active
Bit	Meaning When Set																						
0	Tape volume protection in effect																						
1	No duplicate data set protection in effect																						
2	DASD volume protection in effect																						
3	Reserved																						
4	RACROUTE REQUEST=FASTAUTH preprocessing exit routine (ICHRFX01) is active																						
5	RACROUTE REQUEST=LIST pre- and postprocessing exit routine is active																						
6	RACROUTE REQUEST=LIST selection exit routine is active																						
7	RACROUTE REQUEST=DEFINE postprocessing exit routine is active																						
106	6A	RCD81AOP	1	binary	Options indicators: <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Log all users</td> </tr> <tr> <td>1</td> <td>Log all groups</td> </tr> <tr> <td>2</td> <td>Log data set class</td> </tr> <tr> <td>3</td> <td>Log tape volume class</td> </tr> <tr> <td>4</td> <td>Log DASD volume class</td> </tr> <tr> <td>5</td> <td>Log terminal class</td> </tr> <tr> <td>6</td> <td>Log command violations</td> </tr> <tr> <td>7</td> <td>Log special users</td> </tr> </tbody> </table>	Bit	Meaning When Set	0	Log all users	1	Log all groups	2	Log data set class	3	Log tape volume class	4	Log DASD volume class	5	Log terminal class	6	Log command violations	7	Log special users
Bit	Meaning When Set																						
0	Log all users																						
1	Log all groups																						
2	Log data set class																						
3	Log tape volume class																						
4	Log DASD volume class																						
5	Log terminal class																						
6	Log command violations																						
7	Log special users																						
107	6B	RCD81TMO	1	binary	Options indicators: <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Terminal authorization checking in effect</td> </tr> <tr> <td>1</td> <td>UACC for undefined terminals is NONE</td> </tr> <tr> <td>2</td> <td>REALDSN is in effect</td> </tr> <tr> <td>3</td> <td>JES-XBMALLRACF is in effect</td> </tr> <tr> <td>4</td> <td>JES-EARLYVERIFY is in effect</td> </tr> <tr> <td>5</td> <td>JES-BATCHALLRACF is in effect</td> </tr> <tr> <td>6</td> <td>RACROUTE REQUEST=FASTAUTH postprocessing exit is active</td> </tr> <tr> <td>7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Meaning When Set	0	Terminal authorization checking in effect	1	UACC for undefined terminals is NONE	2	REALDSN is in effect	3	JES-XBMALLRACF is in effect	4	JES-EARLYVERIFY is in effect	5	JES-BATCHALLRACF is in effect	6	RACROUTE REQUEST=FASTAUTH postprocessing exit is active	7	Reserved
Bit	Meaning When Set																						
0	Terminal authorization checking in effect																						
1	UACC for undefined terminals is NONE																						
2	REALDSN is in effect																						
3	JES-XBMALLRACF is in effect																						
4	JES-EARLYVERIFY is in effect																						
5	JES-BATCHALLRACF is in effect																						
6	RACROUTE REQUEST=FASTAUTH postprocessing exit is active																						
7	Reserved																						
108	6C	RCD81PIV	1	binary	Maximum password interval																		
109	6D	RCD81MFG	1	binary	Model flags: <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Model—GDG</td> </tr> <tr> <td>1</td> <td>Model—USER</td> </tr> <tr> <td>2</td> <td>Model—GROUP</td> </tr> <tr> <td>3-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Meaning When Set	0	Model—GDG	1	Model—USER	2	Model—GROUP	3-7	Reserved								
Bit	Meaning When Set																						
0	Model—GDG																						
1	Model—USER																						
2	Model—GROUP																						
3-7	Reserved																						
110	6E	RCD81MSF	1	binary	Miscellaneous processing flags: <table border="0"> <thead> <tr> <th>Bit</th> <th>Meaning When Set</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>GRPLIST active</td> </tr> <tr> <td>1</td> <td>Generic profile checking in effect for data set</td> </tr> <tr> <td>2</td> <td>GENCMD in effect for data set class</td> </tr> <tr> <td>3</td> <td>ADSP attribute bypassed</td> </tr> <tr> <td>4-7</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Meaning When Set	0	GRPLIST active	1	Generic profile checking in effect for data set	2	GENCMD in effect for data set class	3	ADSP attribute bypassed	4-7	Reserved						
Bit	Meaning When Set																						
0	GRPLIST active																						
1	Generic profile checking in effect for data set																						
2	GENCMD in effect for data set class																						
3	ADSP attribute bypassed																						
4-7	Reserved																						

Offsets

Dec.	Hex.	Name	Length	Format	Description
111	6F	RCD81IFG	1	binary	Internal processing flags: Bit Meaning When Set 0 The SETROPTS command caused RACFRW to generate this record 1 The RVARY command caused RACFRW to generate this record 2 RACF was varied active by RVARY command 3 This record is incomplete (truncated) 4 RVARY SWITCH was issued 5-7 Reserved
112	70	RCD81QL	8	char	Single level data set name prefix
120	78	RCD81A02	1	binary	Options indicator Bit Meaning When Set 0 Log OPERATIONS user 1-7 Reserved 2 RACF was varied active by RVARY command.
121	79	RCD81OP4	1	binary	Options indicators Bit Meaning When Set 0 Tape DSN active 1 PROTECTALL active 2 PROTECTALL warning 3 Erase-on-scratch 4 Erase by SECLEVEL 5 Erase all files 6-7 Reserved
122	7A	RCD81OP5	1	binary	Options indicators Bit Meaning When Set 0 Program control active 1 ACEE compression/expansion exit active 2 RACROUTE REQUEST=FASTAUTH postprocessing exit ICHRFX04 active 3 RACROUTE REQUEST=FASTAUTH postprocessing exit ICHRFX04 active 4-7 Reserved
124	7C	RCD81RPD	2	binary	Data set retention period
126	7E	RCD81SLV	1	char	SECLEVEL number
127	7F	RCD81SLC	1	binary	SECLEVEL for auditing number
128	80	RCD81BOP	1	binary	B1 security options Bit Meaning When Set 0 SECLABELCONTROL active 1 CATDSNS active 2 MLQUIET active 3 MLSTABLE active 4 MLS active 5 MLACTIVE active 6 GENERICOWNER active 7 SECLABELAUDIT active
129	81	RCD81SIN	2	binary	SESSION INTERVAL
131	83	RCD81SYS	8	char	User ID for JES SYSOUTNAME
139	8B	RCD81UND	8	char	User ID for JES undefined user

Reformatted SMF Records

Offsets

Dec.	Hex.	Name	Length	Format	Description
147	93	RCD81BOX	1	binary	B1 security options extension byte
					Bit Meaning When Set 0 COMPATMODE 1 CATDSNS failures 2 MLS failures 3 MLACTIVE failures 4-7 Reserved
148	94	RCD81PRI	3	EBCDIC	Primary language default
151	97	RCD81SEC	3	EBCDIC	Secondary language default
Variable Relocate Section Map					
+0	+0	RCDDTYPE	1	binary	Data type
+1	+1	RCDDLGT	1	binary	Length of data that follows
+2	+2	RCDDATA	variable	mixed	Data

Note: Only data types (SMF80DTP) 21, 30, 32, 34, 35 or 36 are generated for a reformatted status record. See “Table of Relocate Section Variable Data” on page 54 earlier in this chapter for a further explanation of these data types.

Chapter 6. RACF SMF Data Unload Utility (IRRADU00)

IRRADU00 Record Format

The following sections contain a detailed description of the records that are produced by the RACF SMF data unload utility. The output of the utility is a series of records that represents the security relevant SMF data that is the input to the utility. These records are in a format suitable for export to the relational data manager of an installation's choice.

Each record that is produced by the RACF SMF data unload utility consists of two parts:

1. A header section, which contains common information such as the date and time stamp, user ID, and system identification
2. An event-specific information section

Each row in the tabular description of the records that are produced by the utility contains five pieces of information:

1. Descriptive name for the field
2. Type of field
 - Char** Character data
 - Integer** EBCDIC numeric data
 - Time** A time value, in the form *hh:mm:ss*
 - Date** A date value, in the form *yyyy-mm-dd*
 - Yes/No** Flag data, having the value YES or NO
3. Starting position for the field
4. Ending position for the field
5. Free-form description of the field, which may contain the valid value constraints.

In some cases, the input SMF record does not contain all of the data that are indicated in the output record mappings shown in the following sections. In these cases, IRRADU00 places blanks in the fields.

For the audit records created for RACF commands, the exact order and format of the unloaded keywords and operands from the commands, (contained within the fields whose names end with "_SPECIFIED", "_IGNORED", and "_FAILED,") are not part of the programming interface.

The Format of the Header Portion of the Unloaded SMF Records

Table 2 on page 114 describes the format of the header portion of the record. RACF constructs the header portion of the record from the SMF record. Because each of the SMF record types that IRRADU00 processes contain different data, some fields of the header portion of the unloaded SMF record contain blanks. For example, JOBINIT records that are created from type 30 SMF records have blanks for these fields:

- INIT_VIOLATION
- INIT_USR_NDFND
- INIT_USER_WARNING
- All of the INIT_AUTH_ fields
- All of the INIT_LOG_ fields
- INIT_TERM_LEVEL
- INIT_BACKOUT_FAIL
- INIT_PROF_SAME
- INIT_TERM

SMF Data Unload—IRRADU00

- INIT_READ_TIME
- INIT_READ_DATE
- INIT_USR_SECL
- INIT_RACF_VERSION

The <col_id> string is replaced by the column identifier for each record created. See Table 3 on page 116 for a list of the valid column identifiers.

Table 2. Format of the Header Portion of the Unloaded SMF Records

Field Name	Type	Length	Position		Comments
			Start	End	
<col_id>_EVENT_TYPE	Char	8	1	8	Type of event that is described. Valid values are shown in Table 3 on page 116. A numeric value indicates that the event code was not translated. Only header information is created for records that have an untranslated event code.
<col_id>_EVENT_QUAL	Char	8	10	17	A qualification of the type of event that is being described. Valid values are shown in the tables that accompany each of the record extension descriptions.
<col_id>_TIME_WRITTEN	Time	8	19	26	Time that the record was written to SMF.
<col_id>_DATE_WRITTEN	Date	10	28	37	Date that the record was written to SMF.
<col_id>_SYSTEM_SMFID	Char	4	39	42	SMF system ID of the system from which the record originates.
<col_id>_VIOLATION	Yes/No	4	44	47	Does this record represent a violation?
<col_id>_USER_NDFND	Yes/No	4	49	52	Was this user not defined to RACF?
<col_id>_USER_WARNING	Yes/No	4	54	57	Was this record created because of WARNING?
<col_id>_EVT_USER_ID	Char	8	59	66	User ID associated with the event.
<col_id>_EVT_GRP_ID	Char	8	68	75	Group name associated with the event.
<col_id>_AUTH_NORMAL	Yes/No	4	77	80	Was normal authority checking a reason for access being allowed?
<col_id>_AUTH_SPECIAL	Yes/No	4	82	85	Was special authority checking a reason for access being allowed?
<col_id>_AUTH_OPER	Yes/No	4	87	90	Was operations authority checking a reason for access being allowed?
<col_id>_AUTH_AUDIT	Yes/No	4	92	95	Was auditor authority checking a reason for access being allowed?
<col_id>_AUTH_EXIT	Yes/No	4	97	100	Was exit checking a reason for access being allowed?
<col_id>_AUTH_FAILSFT	Yes/No	4	102	105	Was failsoft checking a reason for access being allowed?
<col_id>_AUTH_BYPASS	Yes/No	4	107	110	Was the use of the user ID *BYPASS* a reason for access being allowed?
<col_id>_AUTH_TRUSTED	Yes/No	4	112	115	Was trusted authority checking a reason for access being allowed?
<col_id>_LOG_CLASS	Yes/No	4	117	120	Was SETR AUDIT(class) checking a reason for this event to be recorded?
<col_id>_LOG_USER	Yes/No	4	122	125	Was auditing requested for this user?
<col_id>_LOG_SPECIAL	Yes/No	4	127	130	Was auditing requested for access granted due to the SPECIAL privilege?
<col_id>_LOG_ACCESS	Yes/No	4	132	135	Did the profile indicate audit, or did FAILSOFT processing allow access, or did the RACHECK exit indicate auditing?
<col_id>_LOG_RACINIT	Yes/No	4	137	140	Did the RACINIT fail?
<col_id>_LOG_ALWAYS	Yes/No	4	142	145	Is this command always audited?

Table 2. Format of the Header Portion of the Unloaded SMF Records (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
<col_id>_LOG_CMDVIOL	Yes/No	4	147	150	Was this event audited due to CMDVIOL?
<col_id>_LOG_GLOBAL	Yes/No	4	152	155	Was this event audited due to GLOBALAUDIT?
<col_id>_TERM_LEVEL	Integer	3	157	159	The terminal level associated with this audit record.
<col_id>_BACKOUT_FAIL	Yes/No	4	161	164	Did RACF fail in backing out the data?
<col_id>_PROF_SAME	Yes/No	4	166	169	Did a RACF error cause the profile to not be changed?
<col_id>_TERM	Char	8	171	178	The terminal associated with the event.
<col_id>_JOB_NAME	Char	8	180	187	The job name associated with the event.
<col_id>_READ_TIME	Time	8	189	196	The time that the job entered the system.
<col_id>_READ_DATE	Date	10	198	207	The date that the job entered the system.
<col_id>_SMF_USER_ID	Char	8	209	216	User ID from SMF common area. This value is managed by SMF and the SMF processing exits.
<col_id>_LOG_LEVEL	Yes/No	4	218	221	Was this event audited due to SECLEVEL auditing?
<col_id>_LOG_VMEVENT	Yes/No	4	223	226	Was this event audited due to VMEVENT auditing?
<col_id>_LOG_LOGOPT	Yes/No	4	228	231	Was this event audited due to SETR LOGOPTIONS auditing?
<col_id>_LOG_SECL	Yes/No	4	233	236	Was this event audited due to SETR SECLABELAUDIT auditing?
<col_id>_LOG_COMPATM	Yes/No	4	238	241	Was this event audited due to SETR COMPATMODE auditing?
<col_id>_LOG_APPLAUD	Yes/No	4	243	246	Was this event audited due to SETR APPLAUDIT?
<col_id>_LOG_NONOMVS	Yes/No	4	248	251	Did this user try to use z/OS UNIX without being defined as a z/OS UNIX user (that is, is the user's OMVS segment in the RACF database missing)?
<col_id>_LOG_OMVSNPRV	Yes/No	4	253	256	The service that was requested requires that the user be the z/OS UNIX super-user.
<col_id>_AUTH_OMVSSU	Yes/No	4	258	261	Was the z/OS UNIX superuser authority used to grant the request?
<col_id>_AUTH_OMVSSYS	Yes/No	4	263	266	Was the request granted because the requester was z/OS UNIX itself?
<col_id>_USR_SECL	Char	8	268	275	The SECLABEL associated with this user.
<col_id>_RACF_VERSION	Char	4	277	280	The version of RACF on the system which audited the event.

Event Codes

The RACF SMF data unload utility creates records that represent the audit information for each type of auditable event. Table 3 on page 116 contains a list of all of the supported event codes.

COLUMN NAME	DESCRIPTION
Event Code Name	Name of the event code
Column ID (Col ID)	Shortened name that is used in the column name of fields that are a part of the event code record
Event Code	The number assigned to this event code by RACF
Description	A description of the event code.

SMF Data Unload—IRRADU00

Where Described Where you can find the record definitions.

Table 3. Event Codes and Descriptions

Event Code Name	Col ID	Event Code	Description	Where Described
JOBINIT	INIT	01	Job initiation	"The Format of the JOBINIT Record Extension" on page 119
ACCESS	ACC	02	Resource access, other than file or directory.	"The Format of the ACCESS Record Extension" on page 121
ADDVOL	ADV	03	ADDVOL/CHGVOL	"The Format of the ADDVOL Record Extension" on page 124
RENAMEDS	REN	04	Rename data set, SFS file, or SFS directory	"The Format of the RENAMEDS Record Extension" on page 125
DELRES	DELR	05	Delete resource	"The Format of the DELRES Record Extension" on page 127
DELVOL	DELV	06	Delete volume	"The Format of the DELVOL Record Extension" on page 128
DEFINE	DEF	07	Define resource	"The Format of the DEFINE Record Extension" on page 129
ADDSD	AD	08	ADDSD command	"The Format of the ADDSD Record Extension" on page 131
ADDGROUP	AG	09	ADDGROUP command	"The Format of the ADDGROUP Record Extension" on page 132
ADDUSER	AU	10	ADDUSER command	"The Format of the ADDUSER Record Extension" on page 134
ALTDSD	ALD	11	ALTDSD command	"The Format of the ALTDSD Record Extension" on page 135
ALTGROUP	ALG	12	ALTGROUP command	"The Format of the ALTGROUP Record Extension" on page 136
ALTUSER	ALU	13	ALTUSER command	"The Format of the ALTUSER Record Extension" on page 138
CONNECT	CON	14	CONNECT command	"The Format of the CONNECT Record Extension" on page 139
DELSD	DELD	15	DELSD command	"The Format of the DELSD Record Extension" on page 140
DELGROUP	DELG	16	DELGROUP command	"The Format of the DELGROUP Record Extension" on page 142
DELUSER	DELU	17	DELUSER command	"The Format of the DELUSER Record Extension" on page 143
PASSWORD	PWD	18	PASSWORD command	"The Format of the PASSWORD Record Extension" on page 144
PERMIT	PERM	19	PERMIT command	"The Format of the PERMIT Record Extension" on page 145
RALTER	RALT	20	RALTER command	"The Format of the RALTER Record Extension" on page 146
RDEFINE	RDEF	21	RDEFINE command	"The Format of the RDEFINE Record Extension" on page 148
RDELETE	RDEL	22	RDELETE command	"The Format of the RDELETE Record Extension" on page 149
REMOVE	REM	23	REMOVE command	"The Format of the REMOVE Record Extension" on page 150
SETROPTS	SETR	24	SETROPTS command	"The Format of the SETROPTS Record Extension" on page 151
RVARY	RVAR	25	RVARY command	"The Format of the RVARY Record Extension" on page 153

Table 3. Event Codes and Descriptions (continued)

Event Code Name	Col ID	Event Code	Description	Where Described
APPCLU	APPC	26	APPC session	"The Format of the APPCLU Record Extension" on page 154
GENERAL	GEN	27	General purpose	"The Format of the General Event Record Extension" on page 155
DIRSRCH	DSCH	28	Directory Search	"The Format of the Directory Search Record Extension" on page 156
DACCESS	DACC	29	Check access to a directory	"The Format of the Check Directory Access Record Extension" on page 158
FACCESS	FACC	30	Check access to file	"The Format of the Check File Access Record Extension" on page 160
CHAUDIT	CAUD	31	Change audit options	"The Format of the Change Audit Record Extension" on page 162
CHDIR	CDIR	32	Change current directory	"The Format of the Change Directory Record Extension" on page 165
CHMOD	CMOD	33	Change file mode	"The Format of the Change File Mode Record Extension" on page 166
CHOWN	COWN	34	Change file ownership	"The Format of the Change File Ownership Record Extension" on page 169
CLRSETID	CSID	35	Clear SETID bits for a file	"The Format of the Clear SETID Bits Record Extension" on page 171
EXESETID	ESID	36	EXEC with SETUID/SETGID	"The Format of the EXEC SETUID/SETGID Record Extension" on page 173
GETPSENT	GPST	37	Get z/OS UNIX process entry	"The Format of the GETPSENT Record Extension" on page 174
INITOEDP	IOEP	38	Initialize z/OS UNIX process	"The Format of the Initialize z/OS UNIX Record Extension" on page 176
TERMOEDP	TOEP	39	z/OS UNIX process complete	"The Format of the z/OS UNIX Process Completion Record" on page 177
KILL	KILL	40	Terminate a process	"The Format of the KILL Record Extension" on page 178
LINK	LINK	41	LINK	"The Format of the LINK Record Extension" on page 180
MKDIR	MDIR	42	Make directory	"The Format of the MKDIR Record Extension" on page 182
MKNOD	MNOD	43	Make node	"The Format of the MKNOD Record Extension" on page 184
MNTFSYS	MFS	44	Mount a file system	"The Format of the Mount File System Record Extension" on page 187
OPENFILE	OPEN	45	Open a new file	"The Format of the OPENFILE Record Extension" on page 189
PTRACE	PTRC	46	PTRACE authority checking	"The Format of the PTRACE Record Extension" on page 192
RENAMEF	RENF	47	Rename file	"The Format of the Rename File Record Extension" on page 193
RMDIR	RDIR	48	Remove directory	"The Format of the RMDIR Record Extension" on page 195
SETEGID	SEGI	49	Set effective z/OS UNIX group identifier (GID).	"The Format of the SETEGID (SET Effective z/OS UNIX Group Identifier (GID) Record Extension" on page 197
SETEUID	SEUI	50	Set effective z/OS UNIX user identifier (UID)	"The Format of the SETEUID (SET Effective z/OS UNIX User Identifier (UID) Record Extension" on page 198

SMF Data Unload—IRRADU00

Table 3. Event Codes and Descriptions (continued)

Event Code Name	Col ID	Event Code	Description	Where Described
SETGID	SGI	51	Set z/OS UNIX group identifier (GID).	"The Format of the SETGID Record Extension" on page 199
SETUID	SUI	52	Set z/OS UNIX user identifier (UID)	"The Format of the SETUID Record Extension" on page 201
SYMLINK	SYML	53	SYMLINK	"The Format of the SYMLINK Record Extension" on page 202
UNLINK	UNL	54	UNLINK	"The Format of the UNLINK Record Extension" on page 204
UMNTFSYS	UFS	55	Unmount file system	"The Format of the Unmount File System Record Extension" on page 206
CHKFOWN	CFOW	56	Check file owner	"The Format of the Check File Owner Record Extension" on page 207
CHKPRIV	CPRV	57	Check privilege	"The Format of the Check Privilege Record Extension" on page 209
OPENSTTY	OSTY	58	Open slave TTY	"The Format of the Open Slave TTY Record Extension" on page 210
RACLINK	RACL	59	RACLINK command	"The Format of the RACLINK Command Record Extension" on page 212
IPCCHK	ICLK	60	Check IPC access	"The Format of the IPCCHK Record Extension" on page 214
IPCGET	IGET	61	IPCGET	"The Format of the IPCGET Record Extension" on page 216
IPCCTL	ICTL	62	IPCCTL	"The Format of the IPCCTL Record Extension" on page 218
SETGROUP	SETG	63	SETGROUP	"The Format of the SETGROUP Record Extension" on page 220
CKOWN2	CKO2	64	CKOWN2	"The Format of the CKOWN2 Record Extension" on page 222
R_AUDIT	ACCR	65	Access Rights	"The Format of the Access Rights Record Extension" on page 223
RACDCERT	RACD	66	RACDCERT command	"The Format of the RACDCERT Command Record Extension" on page 225
INITACEE	INTA	67	InitACEE	"The Format of the InitACEE Record Extension" on page 226
KTICKET	KTKT	68	Grant of initial Kerberos ticket	"The Format of the Network Authentication Service Record Extension" on page 227
RPKIGENC	RPKG	69	Certificate GENCERT request	"The Format of the RPKIGENC Record Extension" on page 228
RPKIEXPT	RPKE	70	Certificate EXPORT request	"The Format of the RPKIEXPT Record Extension" on page 229
PDACCESS	PDAC	71	Policy Director Authorization Services Support access control decision	"The Format of the Policy Director Authorization Services Support Record Extension" on page 231
READATA	RPKR	72		"The Format of the RPKIREAD Record Extension" on page 231
UPDATEREQ	RPKU	73		"The Format of the RPKIUPDR Record Extension" on page 233
UPDATECERT	RPKC	74		"The Format of the RPKIUPDC Record Extension" on page 234
SETFACL	SACL	75	ACL entry changes	"The Format of the SETFACL Record Extension" on page 236

Table 3. Event Codes and Descriptions (continued)

Event Code Name	Col ID	Event Code	Description	Where Described
DELFACL	DACL	76	ACL deletion	"The Format of the DELFACL Record Extension" on page 238

Record Extensions

The sections that follow describe the event-specific information. The extensions reflect the relocate section data for a specific event code. Fields in the event-specific information might contain blanks because not all relocate sections are created for a given event code.

The Format of the JOBINIT Record Extension

Table 4 describes the format of a record that is created by the RACINIT function, which occurs for user logons, batch job initiations, and at other times during the life of a unit of work. These fields are only present on JOBINIT records that are created from SMF type 80 records. JOBINIT records that are created from SMF type 30 records contain blanks in these fields.

Table 4. Format of the Job Initiation Record Extension (Event Code 01)

Field Name	Type	Length	Position		Comments
			Start	End	
INIT_APPL	Char	8	282	289	Application name specified on the RACROUTE REQUEST=AUTH or REQUEST=VERIFY.
INIT_LOGSTR	Char	255	291	545	LOGSTR= data from the RACROUTE
INIT_BAD_JOBNAME	Char	8	547	554	The invalid job name that was processed.
INIT_USER_NAME	Char	20	556	575	The name associated with the user ID.
INIT_UTK_ENCR	Yes/No	4	577	580	Is the UTOKEN associated with this user encrypted?
INIT_UTK_PRE19	Yes/No	4	582	585	Is this a pre-1.9 token?
INIT_UTK_VERPROF	Yes/No	4	587	590	Is the VERIFYX propagation flag set?
INIT_UTK_NJEUNUSR	Yes/No	4	592	595	Is this the NJE undefined user?
INIT_UTK_LOGUSR	Yes/No	4	597	600	Is UAUDIT specified for this user?
INIT_UTK_SPECIAL	Yes/No	4	602	605	Is this a SPECIAL user?
INIT_UTK_DEFAULT	Yes/No	4	607	610	Is this a default token?
INIT_UTK_UNKNUSR	Yes/No	4	612	615	Is this an undefined user?
INIT_UTK_ERROR	Yes/No	4	617	620	Is this user token in error?
INIT_UTK_TRUSTED	Yes/No	4	622	625	Is this user a part of the trusted computing base (TCB)?
INIT_UTK_SESSTYPE	Char	8	627	634	The session type of this session. See <i>z/OS Security Server RACROUTE Macro Reference</i> for a description of the valid values for session type. A null session type results in the unloading of blanks.
INIT_UTK_SURROGAT	Yes/No	4	636	639	Is this a surrogate user?
INIT_UTK_REMOTE	Yes/No	4	641	644	Is this a remote job?
INIT_UTK_PRIV	Yes/No	4	646	649	Is this a privileged user ID?
INIT_UTK_SECL	Char	8	651	658	The SECLABEL of the user.
INIT_UTK_EXECNODE	Char	8	660	667	The execution node of the work.
INIT_UTK_SUSER_ID	Char	8	669	676	The submitting user ID.

SMF Data Unload—IRRADU00

Table 4. Format of the Job Initiation Record Extension (Event Code 01) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
INIT_UTK_SNODE	Char	8	678	685	The submitting node.
INIT_UTK_SGRP_ID	Char	8	687	694	The submitting group name.
INIT_UTK_SPOE	Char	8	696	703	The port of entry.
INIT_UTK_SPCLASS	Char	8	705	712	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
INIT_UTK_USER_ID	Char	8	714	721	User ID associated with the record.
INIT_UTK_GRP_ID	Char	8	723	730	Group name associated with the record.
INIT_UTK_DFT_GRP	Yes/No	4	732	735	Is a default group assigned?
INIT_UTK_DFT_SECL	Yes/No	4	737	740	Is a default SECLABEL assigned?
INIT_APPC_LINK	Char	16	742	757	A key to link together audit record together for a user's APPC transaction processing work.
INIT_UTK_NETW	Char	8	759	766	The port of entry network name.
INIT_RES_NAME	Char	255	768	1022	Resource name.
INIT_CLASS	Char	8	1024	1031	Class name.
INIT_X500_SUBJECT	Char	255	1033	1287	Subject's name associated with this event.
INIT_X500_ISSUER	Char	255	1289	1543	Issuer's name associated with this event.

Event Qualifiers for JOBINIT (Job Initiation) Records

The event qualifiers that may be associated with a JOBINIT event are shown in Table 5.

Table 5. Event Qualifiers for JOBINIT Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	--	Successful initiation (from type 30 record)
TERM	--	Successful termination (from type 30 record)
SUCCESSI	00	Successful initiation.
INVPSWD	01	Not a valid password.
INVGRP	02	Not a valid group.
INVOID	03	Not a valid OIACARD.
INVTerm	04	Not a valid terminal.
INVAPPL	05	Not a valid application.
REVKUSER	06	User has been revoked.
REVKAUTO	07	User automatically revoked.
SUCCEST	08	Successful termination.
UNDFUSER	09	User not defined to RACF.
INSSECL	10	Insufficient SECLABEL.
NASECL	11	Not authorized to SECLABEL.
RACINITI	12	Successful RACINIT initiation.
RACINITD	13	Successful RACINIT deletion.
MOREAUTH	14	More authority required.
RJENAUTH	15	RJE not authorized.
SURROGTI	16	Surrogate class inactive.
SUBNATHU	17	Submitter not authorized by user.

Table 5. Event Qualifiers for JOBINIT Records (continued)

Event Qualifier	Event Qualifier Number	Event Description
SUBNATHS	18	Submitter not authorized by SECLABEL.
USERNJOB	19	User not authorized to the job.
WINSSECL	20	Warning: Insufficient SECLABEL.
WSECLM	21	Warning: SECLABEL missing from job.
WNASECL	22	Warning: Not authorized to SECLABEL.
SECLNCM	23	SECLABELs not compatible.
WSECLNCM	24	Warning: SECLABELs not compatible.
PWDEXPR	25	Current password has expired.
INVNPWD	26	Not a valid new password.
EXITFAIL	27	Failed by installation exit.
GRPARVKD	28	Group access revoked.
OIDREQD	29	OIDCARD required.
NJENAUTH	30	NJE job not authorized.
WUKNUPRP	31	Warning: Undefined user from trusted node propagated.
SUCCESSP	32	Successful initiation using a PassTicket.
PTKTREPL	33	Attempted replay of PassTicket.

The Format of the ACCESS Record Extension

Table 6 describes the format of a record that is created by the access to a resource.

Table 6. Format of the ACCESS Record Extension (Event Code Number 02)

Field Name	Type	Length	Position		Comments
			Start	End	
ACC_RES_NAME	Char	255	282	536	Resource name or old resource name.
ACC_REQUEST	Char	8	538	545	The access authority requested.
ACC_GRANT	Char	8	547	554	The access authority granted.
ACC_LEVEL	Integer	3	556	558	Level of the resource.
ACC_VOL	Char	6	560	565	Volume of the resource.
ACC_OLDVOL	Char	6	567	572	OLDVOL of the resource.
ACC_CLASS	Char	8	574	581	Class name.
ACC_APPL	Char	8	583	590	Application name specified.
ACC_TYPE	Char	8	592	599	Type of resource data. Valid values are "RESOURCE" if ACC_NAME is a generic resource name, and "PROFILE" if ACC_NAME is a generic profile.
ACC_NAME	Char	246	601	846	Resource or profile name.
ACC_OWN_ID	Char	8	848	855	Name of the profile owner.
ACC_LOGSTR	Char	255	857	1111	LOGSTR= data from the RACROUTE.
ACC_RECVR	Char	8	1113	1120	User ID to whom the data is directed (RECVR= on RACROUTE).
ACC_USER_NAME	Char	20	1122	1141	User name from the ACEE.
ACC_SECL	Char	8	1143	1150	SECLABEL of the resource.
ACC_UTK_ENCR	Yes/No	4	1152	1155	Is the UTOKEN associated with this user encrypted?
ACC_UTK_PRE19	Yes/No	4	1157	1160	Is this a pre-1.9 token?

SMF Data Unload—IRRADU00

Table 6. Format of the ACCESS Record Extension (Event Code Number 02) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
ACC_UTK_VERPROF	Yes/No	4	1162	1165	Is the VERIFYX propagation flag set?
ACC_UTK_NJEUNUSR	Yes/No	4	1167	1170	Is this the NJE undefined user?
ACC_UTK_LOGUSR	Yes/No	4	1172	1175	Is UAUDIT specified for this user?
ACC_UTK_SPECIAL	Yes/No	4	1177	1180	Is this a SPECIAL user?
ACC_UTK_DEFAULT	Yes/No	4	1182	1185	Is this a default token?
ACC_UTK_UNKNUSR	Yes/No	4	1187	1190	Is this an undefined user?
ACC_UTK_ERROR	Yes/No	4	1192	1195	Is this user token in error?
ACC_UTK_TRUSTED	Yes/No	4	1197	1200	Is this user a part of the trusted computing base (TCB)?
ACC_UTK_SESSTYPE	Char	8	1202	1209	The session type of this session.
ACC_UTK_SURROGAT	Yes/No	4	1211	1214	Is this a surrogate user?
ACC_UTK_REMOTE	Yes/No	4	1216	1219	Is this a remote job?
ACC_UTK_PRIV	Yes/No	4	1221	1224	Is this a privileged user ID?
ACC_UTK_SECL	Char	8	1226	1233	The SECLABEL of the user.
ACC_UTK_EXECNODE	Char	8	1235	1242	The execution node of the work.
ACC_UTK_SUSER_ID	Char	8	1244	1251	The submitting user ID.
ACC_UTK_SNODE	Char	8	1253	1260	The submitting node.
ACC_UTK_SGRP_ID	Char	8	1262	1269	The submitting group name.
ACC_UTK_SPOE	Char	8	1271	1278	The port of entry.
ACC_UTK_SPCLASS	Char	8	1280	1287	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
ACC_UTK_USER_ID	Char	8	1289	1296	User ID associated with the record.
ACC_UTK_GRP_ID	Char	8	1298	1305	Group name associated with the record.
ACC_UTK_DFT_GRP	Yes/No	4	1307	1310	Is a default group assigned?
ACC_UTK_DFT_SECL	Yes/No	4	1312	1315	Is a default SECLABEL assigned?
ACC_RTK_ENCR	Yes/No	4	1317	1320	Is the RTOKEN associated with this user encrypted?
ACC_RTK_PRE19	Yes/No	4	1322	1325	Is this a pre-1.9 token?
ACC_RTK_VERPROF	Yes/No	4	1327	1330	Is the VERIFYX propagation flag set?
ACC_RTK_NJEUNUSR	Yes/No	4	1332	1335	Is this the NJE undefined user?
ACC_RTK_LOGUSR	Yes/No	4	1337	1340	Is UAUDIT specified for this user?
ACC_RTK_SPECIAL	Yes/No	4	1342	1345	Is this a SPECIAL user?
ACC_RTK_DEFAULT	Yes/No	4	1347	1350	Is this a default token?
ACC_RTK_UNKNUSR	Yes/No	4	1352	1355	Is this an undefined user?
ACC_RTK_ERROR	Yes/No	4	1357	1360	Is this user token in error?
ACC_RTK_TRUSTED	Yes/No	4	1362	1365	Is this user a part of the trusted computing base (TCB)?
ACC_RTK_SESSTYPE	Char	8	1367	1374	The session type of this session.
ACC_RTK_SURROGAT	Yes/No	4	1376	1379	Is this a surrogate user?
ACC_RTK_REMOTE	Yes/No	4	1381	1384	Is this a remote job?
ACC_RTK_PRIV	Yes/No	4	1386	1389	Is this a privileged user ID?
ACC_RTK_SECL	Char	8	1391	1398	The SECLABEL of the user.
ACC_RTK_EXECNODE	Char	8	1400	1407	The execution node of the work.
ACC_RTK_SUSER_ID	Char	8	1409	1416	The submitting user ID.
ACC_RTK_SNODE	Char	8	1418	1425	The submitting node.

Table 6. Format of the ACCESS Record Extension (Event Code Number 02) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
ACC_RTK_SGRP_ID	Char	8	1427	1434	The submitting group name.
ACC_RTK_SPOE	Char	8	1436	1443	The port of entry.
ACC_RTK_SPCLASS	Char	8	1445	1452	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
ACC_RTK_USER_ID	Char	8	1454	1461	User ID associated with the record.
ACC_RTK_GRP_ID	Char	8	1463	1470	Group name associated with the record.
ACC_RTK_DFT_GRP	Yes/No	4	1472	1475	Is a default group assigned?
ACC_RTK_DFT_SECL	Yes/No	4	1477	1480	Is a default SECLABEL assigned?
ACC_APPC_LINK	Char	16	1482	1497	A key to link together audit record together for a user's APPC transaction processing work.
ACC_DCE_LINK	Char	16	1499	1514	Link to connect DCE records that originate from a single DCE request.
ACC_AUTH_TYPE	Char	13	1516	1528	Defines the type of request. Valid values are "SERVER", "AUTH_CLIENT" and "UNAUTH_CLIENT".
ACC_PDS_DSN	Char	44	1530	1573	Partitioned data set name.
ACC_UTK_NETW	Char	8	1575	1582	The port of entry network name.
ACC_RTK_NETW	Char	8	1584	1591	The network name from the RTOKEN.
ACC_X500_SUBJECT	Char	255	1593	1847	Subject's name associated with this event.
ACC_X500_ISSUER	Char	255	1849	2103	Issuer's name associated with this event.

Event Qualifiers for ACCESS Records

The event qualifiers that may be associated with an access event are shown in Table 7.

Table 7. Event Qualifiers for Access Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Successful access.
INSAUTH	01	Insufficient authority.
PRFNFD	02	Profile not found; RACFIND specified on macro.
WARNING	03	Access allowed by WARNING.
FPROTALL	04	Failed by PROTECTALL.
WPROTALL	05	PROTECTALL warning.
INSCATG	06	Insufficient category or level.
INSSECL	07	Insufficient SECLABEL.
WSECLM	08	Warning: SECLABEL missing.
WINSSECL	09	Warning: Insufficient SECLABEL.
WNOTCAT	10	Warning: Data set not cataloged, but was required for authority check.
NOTCAT	11	Data set not cataloged.
PRFNFDAI	12	Profile not found.
WINSCATG	13	Warning: Insufficient category or level.
WNONMAIN	14	Warning: Non-MAIN execution environment detected while in ENHANCED PGMSECURITY mode. Conditional access of EXECUTE-controlled program temporarily allowed.

SMF Data Unload—IRRADU00

Table 7. Event Qualifiers for Access Records (continued)

Event Qualifier	Event Qualifier Number	Event Description
PGMBASIC	15	Conditional access or use of EXECUTE-controlled program allowed through BASIC mode program while in ENHANCED PGMSECURITY mode.

Note: Event qualifiers 14 and 15 can be used by PADS for data set access.

The Format of the ADDVOL Record Extension

Table 8 describes the format of a record that is created by the ADDVOL or CHGVOL operations.

Table 8. Format of the ADDVOL Record Extension (Event Code 03)

Field Name	Type	Length	Position		Comments
			Start	End	
ADV_RES_NAME	Char	255	282	536	Resource name.
ADV_GRANT	Char	8	538	545	The access authority granted.
ADV_LEVEL	Integer	3	547	549	The level of the resource.
ADV_VOL	Char	6	551	556	Volume of the resource.
ADV_OLDVOL	Char	6	558	563	OLDVOL of the resource.
ADV_CLASS	Char	8	565	572	Class name.
ADV_OWN_ID	Char	8	574	581	Name of the profile owner.
ADV_LOGSTR	Char	255	583	837	LOGSTR= data from the RACROUTE
ADV_USER_NAME	Char	20	839	858	User name from the ACEE.
ADV_UTK_ENCR	Yes/No	4	860	863	Is the UTOKEN associated with this user encrypted?
ADV_UTK_PRE19	Yes/No	4	865	868	Is this a pre-1.9 token?
ADV_UTK_VERPROF	Yes/No	4	870	873	Is the VERIFYX propagation flag set?
ADV_UTK_NJEUNUSR	Yes/No	4	875	878	Is this the NJE undefined user?
ADV_UTK_LOGUSR	Yes/No	4	880	883	Is UAUDIT specified for this user?
ADV_UTK_SPECIAL	Yes/No	4	885	888	Is this a SPECIAL user?
ADV_UTK_DEFAULT	Yes/No	4	890	893	Is this a default token?
ADV_UTK_UNKNUSR	Yes/No	4	895	898	Is this an undefined user?
ADV_UTK_ERROR	Yes/No	4	900	903	Is this user token in error?
ADV_UTK_TRUSTED	Yes/No	4	905	908	Is this user a part of the trusted computing base (TCB)?
ADV_UTK_SESSTYPE	Char	8	910	917	The session type of this session.
ADV_UTK_SURROGAT	Yes/No	4	919	922	Is this a surrogate user?
ADV_UTK_REMOTE	Yes/No	4	924	927	Is this a remote job?
ADV_UTK_PRIV	Yes/No	4	929	932	Is this a privileged user ID?
ADV_UTK_SECL	Char	8	934	941	The SECLABEL of the user.
ADV_UTK_EXECNODE	Char	8	943	950	The execution node of the work.
ADV_UTK_SUSER_ID	Char	8	952	959	The submitting user ID.
ADV_UTK_SNODE	Char	8	961	968	The submitting node.
ADV_UTK_SGRP_ID	Char	8	970	977	The submitting group name.
ADV_UTK_SPOE	Char	8	979	986	The port of entry.
ADV_UTK_SPCLASS	Char	8	988	995	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".

Table 8. Format of the ADDVOL Record Extension (Event Code 03) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
ADV_UTK_USER_ID	Char	8	997	1004	User ID associated with the record.
ADV_UTK_GRP_ID	Char	8	1006	1013	Group name associated with the record.
ADV_UTK_DFT_GRP	Yes/No	4	1015	1018	Is a default group assigned?
ADV_UTK_DFT_SECL	Yes/No	4	1020	1023	Is a default SECLABEL assigned?
ADV_APPC_LINK	Char	16	1025	1040	Key to link together APPC records.
ADV_SPECIFIED	Char	1024	1042	2065	RRSF information.
ADV_UTK_NETW	Char	8	2067	2074	The port of entry network name.
ADV_X500_SUBJECT	Char	255	2076	2330	Subject's name associated with this event.
ADV_X500_ISSUER	Char	255	2332	2586	Issuer's name associated with this event.

Event Qualifiers for ADDVOL (Add Volume/Change Volume) Records

The event qualifiers that may be associated with an ADDVOL event are shown in Table 9.

Table 9. Event Qualifiers for Add Volume/Change Volume Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	The volume was successfully added or changed.
INSAUTH	01	Insufficient authority.
INSSECL	02	Insufficient SECLABEL authority.
LESSSPEC	03	A less-specific profile exists with a different SECLABEL.

The Format of the RENAMEDS Record Extension

Table 10 describes the format of a record that is created by the rename data set, rename SFS file, or rename SFS directory operation.

Table 10. Format of the RENAMEDS Record Extension (Event Code 04)

Field Name	Type	Length	Position		Comments
			Start	End	
REN_RES_NAME	Char	255	282	536	Old resource name.
REN_NEW_RES_NAME	Char	255	538	792	New Resource name.
REN_LEVEL	Integer	3	794	796	The level of the resource.
REN_VOL	Char	6	798	803	Volume of the resource.
REN_CLASS	Char	8	805	812	Class name.
REN_OWN_ID	Char	8	814	821	Name of the profile owner.
REN_LOGSTR	Char	255	823	1077	LOGSTR= data from the RACROUTE
REN_USER_NAME	Char	20	1079	1098	User name from the ACEE.
REN_UTK_ENCR	Yes/No	4	1100	1103	Is the UTOKEN associated with this user encrypted?
REN_UTK_PRE19	Yes/No	4	1105	1108	Is this a pre-1.9 token?
REN_UTK_VERPROF	Yes/No	4	1110	1113	Is the VERIFYX propagation flag set?
REN_UTK_NJEUNUSR	Yes/No	4	1115	1118	Is this the NJE undefined user?
REN_UTK_LOGUSR	Yes/No	4	1120	1123	Is UAUDIT specified for this user?
REN_UTK_SPECIAL	Yes/No	4	1125	1128	Is this a SPECIAL user?

SMF Data Unload—IRRADU00

Table 10. Format of the RENAMEDS Record Extension (Event Code 04) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
REN_UTK_DEFAULT	Yes/No	4	1130	1133	Is this a default token?
REN_UTK_UNKNUSR	Yes/No	4	1135	1138	Is this an undefined user?
REN_UTK_ERROR	Yes/No	4	1140	1143	Is this user token in error?
REN_UTK_TRUSTED	Yes/No	4	1145	1148	Is this user a part of the trusted computing base (TCB)?
REN_UTK_SESSTYPE	Char	8	1150	1157	The session type of this session.
REN_UTK_SURROGAT	Yes/No	4	1159	1162	Is this a surrogate user?
REN_UTK_REMOTE	Yes/No	4	1164	1167	Is this a remote job?
REN_UTK_PRIV	Yes/No	4	1169	1172	Is this a privileged user ID?
REN_UTK_SECL	Char	8	1174	1181	The SECLABEL of the user.
REN_UTK_EXECNODE	Char	8	1183	1190	The execution node of the work.
REN_UTK_SUSER_ID	Char	8	1192	1199	The submitting user ID.
REN_UTK_SNODE	Char	8	1201	1208	The submitting node.
REN_UTK_SGRP_ID	Char	8	1210	1217	The submitting group name.
REN_UTK_SPOE	Char	8	1219	1226	The port of entry.
REN_UTK_SPCLASS	Char	8	1228	1235	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
REN_UTK_USER_ID	Char	8	1237	1244	User ID associated with the record.
REN_UTK_GRP_ID	Char	8	1246	1253	Group name associated with the record.
REN_UTK_DFT_GRP	Yes/No	4	1255	1258	Is a default group assigned?
REN_UTK_DFT_SECL	Yes/No	4	1260	1263	Is a default SECLABEL assigned?
REN_APPC_LINK	Char	16	1265	1280	Key to link together APPC records.
REN_SPECIFIED	Char	1024	1282	2305	RRSF information.
REN_UTK_NETW	Char	8	2307	2314	The port of entry network name.
REN_X500_SUBJECT	Char	255	2316	2570	Subject's name associated with this event.
REN_X500_ISSUER	Char	255	2572	2826	Issuer's name associated with this event.

Event Qualifiers for RENAMEDS Records

The event qualifiers that may be associated with a RENAMEDS event are shown in Table 11.

Table 11. Event Qualifiers for RENAMEDS Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Successful rename.
INVGRP	01	Invalid group.
NOTINGRP	02	User not in group.
INSAUTH	03	Insufficient authority.
ALRDEFD	04	Resource already defined.
NOTRACF	05	User is not RACF-defined.
NOTPROT	06	Resource not protected.
WNOTPROT	07	Warning: Resource not
NOT2RACF	08	User in second qualifier is not RACF-defined.
LESSSPEC	09	A less-specific profile exists with a different SECLABEL.

Table 11. Event Qualifiers for RENAMEDS Records (continued)

Event Qualifier	Event Qualifier Number	Event Description
INSSECL	10	Insufficient SECLABEL authority.
RSNSECL	11	Resource not protected by SECLABEL.
NMNSECL	12	New name not protected by SECLABEL.
NODOMIN	13	New SECLABEL must dominate old SECLABEL.
WINSSECL	14	Warning: Insufficient SECLABEL authority.
WRNSECL	15	Warning: Resource not protected by SECLABEL.
WNMNSECL	16	Warning: New name not protected by SECLABEL.
WNODOMIN	17	Warning: New SECLABEL must dominate old SECLABEL.

The Format of the DELRES Record Extension

Table 12 describes the format of a record that is created by the delete resource operation.

Table 12. Format of the DELRES Record Extension (Event Code 05)

Field Name	Type	Length	Position		Comments
			Start	End	
DELR_RES_NAME	Char	255	282	536	Old resource name.
DELR_LEVEL	Integer	3	538	540	The level of the resource.
DELR_VOL	Char	6	542	547	Volume of the resource.
DELR_CLASS	Char	8	549	556	Class name.
DELR_OWN_ID	Char	8	558	565	Name of the profile owner.
DELR_LOGSTR	Char	255	567	821	LOGSTR= data from the RACROUTE
DELR_USER_NAME	Char	20	823	842	User name from the ACEE.
DELR_UTK_ENCR	Yes/No	4	844	847	Is the UTOKEN associated with this user encrypted?
DELR_UTK_PRE19	Yes/No	4	849	852	Is this a pre-1.9 token?
DELR_UTK_VERPROF	Yes/No	4	854	857	Is the VERIFYX propagation flag set?
DELR_UTK_NJEUNUSR	Yes/No	4	859	862	Is this the NJE undefined user?
DELR_UTK_LOGUSR	Yes/No	4	864	867	Is UAUDIT specified for this user?
DELR_UTK_SPECIAL	Yes/No	4	869	872	Is this a SPECIAL user?
DELR_UTK_DEFAULT	Yes/No	4	874	877	Is this a default token?
DELR_UTK_UNKNUSR	Yes/No	4	879	882	Is this an undefined user?
DELR_UTK_ERROR	Yes/No	4	884	887	Is this user token in error?
DELR_UTK_TRUSTED	Yes/No	4	889	892	Is this user a part of the trusted computing base (TCB)?
DELR_UTK_SESSTYPE	Char	8	894	901	The session type of this session.
DELR_UTK_SURROGAT	Yes/No	4	903	906	Is this a surrogate user?
DELR_UTK_REMOTE	Yes/No	4	908	911	Is this a remote job?
DELR_UTK_PRIV	Yes/No	4	913	916	Is this a privileged user ID?
DELR_UTK_SECL	Char	8	918	925	The SECLABEL of the user.
DELR_UTK_EXECNODE	Char	8	927	934	The execution node of the work.
DELR_UTK_SUSER_ID	Char	8	936	943	The submitting user ID.
DELR_UTK_SNODE	Char	8	945	952	The submitting node.
DELR_UTK_SGRP_ID	Char	8	954	961	The submitting group name.

SMF Data Unload—IRRADU00

Table 12. Format of the DELRES Record Extension (Event Code 05) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
DELR_UTK_SPOE	Char	8	963	970	The port of entry.
DELR_UTK_SPCCLASS	Char	8	972	979	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
DELR_UTK_USER_ID	Char	8	981	988	User ID associated with the record.
DELR_UTK_GRP_ID	Char	8	990	997	Group name associated with the record.
DELR_UTK_DFT_GRP	Yes/No	4	999	1002	Is a default group assigned?
DELR_UTK_DFT_SECL	Yes/No	4	1004	1007	Is a default SECLABEL assigned?
DELR_APPC_LINK	Char	16	1009	1024	Key to link together APPC records.
DELR_SPECIFIED	Char	1024	1026	2049	RRSF information.
DELR_UTK_NETW	Char	8	2051	2058	The port of entry network name.
DELR_X500_SUBJECT	Char	255	2060	2314	Subject's name associated with this event.
DELR_X500_ISSUER	Char	255	2316	2570	Issuer's name associated with this event.

Event Qualifiers for DELRES (Delete Resource) Records

The event qualifiers that may be associated with an DELRES event are shown in Table 13.

Table 13. Event Qualifiers for Delete Resource Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	The resource was successfully deleted.
NOTFOUND	01	Resource not found.
INVVOL	02	Invalid volume.

The Format of the DELVOL Record Extension

Table 14 describes the format of a record that is created by the delete resource operation.

Table 14. Format of the DELVOL Record Extension (Event Code 06)

Field Name	Type	Length	Position		Comments
			Start	End	
DELV_RES_NAME	Char	255	282	536	Old resource name.
DELV_LEVEL	Integer	3	538	540	The level of the resource.
DELV_VOL	Char	6	542	547	Volume of the resource.
DELV_CLASS	Char	8	549	556	Class name.
DELV_OWN_ID	Char	8	558	565	Name of the profile owner.
DELV_LOGSTR	Char	255	567	821	LOGSTR= data from the RACROUTE
DELV_USER_NAME	Char	20	823	842	User name.
DELV_UTK_ENCR	Yes/No	4	844	847	Is the UTOKEN associated with this user encrypted?
DELV_UTK_PRE19	Yes/No	4	849	852	Is this a pre-1.9 token?
DELV_UTK_VERPROF	Yes/No	4	854	857	Is the VERIFYX propagation flag set?
DELV_UTK_NJEUNUSR	Yes/No	4	859	862	Is this the NJE undefined user?
DELV_UTK_LOGUSR	Yes/No	4	864	867	Is UAUDIT specified for this user?
DELV_UTK_SPECIAL	Yes/No	4	869	872	Is this a SPECIAL user?

Table 14. Format of the DELVOL Record Extension (Event Code 06) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
DELV_UTK_DEFAULT	Yes/No	4	874	877	Is this a default token?
DELV_UTK_UNKNUSR	Yes/No	4	879	882	Is this an undefined user?
DELV_UTK_ERROR	Yes/No	4	884	887	Is this user token in error?
DELV_UTK_TRUSTED	Yes/No	4	889	892	Is this user a part of the trusted computing base (TCB)?
DELV_UTK_SESSTYPE	Char	8	894	901	The session type of this session.
DELV_UTK_SURROGAT	Yes/No	4	903	906	Is this a surrogate user?
DELV_UTK_REMOTE	Yes/No	4	908	911	Is this a remote job?
DELV_UTK_PRIV	Yes/No	4	913	916	Is this a privileged user ID?
DELV_UTK_SECL	Char	8	918	925	The SECLABEL of the user.
DELV_UTK_EXECNODE	Char	8	927	934	The execution node of the work.
DELV_UTK_SUSER_ID	Char	8	936	943	The submitting user ID.
DELV_UTK_SNODE	Char	8	945	952	The submitting node.
DELV_UTK_SGRP_ID	Char	8	954	961	The submitting group name.
DELV_UTK_SPOE	Char	8	963	970	The port of entry.
DELV_UTK_SPCLASS	Char	8	972	979	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
DELV_UTK_USER_ID	Char	8	981	988	User ID associated with the record.
DELV_UTK_GRP_ID	Char	8	990	997	Group name associated with the record.
DELV_UTK_DFT_GRP	Yes/No	4	999	1002	Is a default group assigned?
DELV_UTK_DFT_SECL	Yes/No	4	1004	1007	Is a default SECLABEL assigned?
DELV_APPC_LINK	Char	16	1009	1024	Key to link together APPC records.
DELV_SPECIFIED	Char	1024	1026	2049	RRSF information.
DELV_UTK_NETW	Char	8	2051	2058	The port of entry network name.
DELV_X500_SUBJECT	Char	255	2060	2314	Subject's name associated with this event.
DELV_X500_ISSUER	Char	255	2316	2570	Issuer's name associated with this event.

Event Qualifiers for DELVOL (Delete Volume) Records

The event qualifier that may be associated with an DELVOL event is shown in Table 15.

Table 15. Event Qualifiers for Delete Volume Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	The volume was successfully deleted.

The Format of the DEFINE Record Extension

Table 16 describes the format of a record that is created by the define resource operation.

Table 16. Format of the DEFINE Record Extension (Event Code 07)

Field Name	Type	Length	Position		Comments
			Start	End	
DEF_RES_NAME	Char	255	282	536	Old resource name.
DEF_LEVEL	Integer	3	538	540	The level of the resource.

SMF Data Unload—IRRADU00

Table 16. Format of the DEFINE Record Extension (Event Code 07) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
DEF_VOL	Char	6	542	547	Volume of the resource.
DEF_CLASS	Char	8	549	556	Class name.
DEF_MODEL_NAME	Char	255	558	812	Name of the model profile.
DEF_MODEL_VOL	Char	6	814	819	Volser of the model profile.
DEF_OWN_ID	Char	8	821	828	Owner of the profile.
DEF_LOGSTR	Char	255	830	1084	LOGSTR= data from the RACROUTE
DEF_USER_NAME	Char	20	1086	1105	User name.
DEF_UTK_ENCR	Yes/No	4	1107	1110	Is the UTOKEN associated with this user encrypted?
DEF_UTK_PRE19	Yes/No	4	1112	1115	Is this a pre-1.9 token?
DEF_UTK_VERPROF	Yes/No	4	1117	1120	Is the VERIFYX propagation flag set?
DEF_UTK_NJEUNUSR	Yes/No	4	1122	1125	Is this the NJE undefined user?
DEF_UTK_LOGUSR	Yes/No	4	1127	1130	Is UAUDIT specified for this user?
DEF_UTK_SPECIAL	Yes/No	4	1132	1135	Is this a SPECIAL user?
DEF_UTK_DEFAULT	Yes/No	4	1137	1140	Is this a default token?
DEF_UTK_UNKNUSR	Yes/No	4	1142	1145	Is this an undefined user?
DEF_UTK_ERROR	Yes/No	4	1147	1150	Is this user token in error?
DEF_UTK_TRUSTED	Yes/No	4	1152	1155	Is this user a part of the trusted computing base (TCB)?
DEF_UTK_SESSTYPE	Char	8	1157	1164	The session type of this session.
DEF_UTK_SURROGAT	Yes/No	4	1166	1169	Is this a surrogate user?
DEF_UTK_REMOTE	Yes/No	4	1171	1174	Is this a remote job?
DEF_UTK_PRIV	Yes/No	4	1176	1179	Is this a privileged user ID?
DEF_UTK_SECL	Char	8	1181	1188	The SECLABEL of the user.
DEF_UTK_EXECNODE	Char	8	1190	1197	The execution node of the work.
DEF_UTK_SUSER_ID	Char	8	1199	1206	The submitting user ID.
DEF_UTK_SNODE	Char	8	1208	1215	The submitting node.
DEF_UTK_SGRP_ID	Char	8	1217	1224	The submitting group name.
DEF_UTK_SPOE	Char	8	1226	1233	The port of entry.
DEF_UTK_SPCLASS	Char	8	1235	1242	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
DEF_UTK_USER_ID	Char	8	1244	1251	User ID associated with the record.
DEF_UTK_GRP_ID	Char	8	1253	1260	Group name associated with the record.
DEF_UTK_DFT_GRP	Yes/No	4	1262	1265	Is a default group assigned?
DEF_UTK_DFT_SECL	Yes/No	4	1267	1270	Is a default SECLABEL assigned?
DEF_APPC_LINK	Char	16	1272	1287	Key to link together APPC records.
DEF_SPECIFIED	Char	1024	1289	2312	RRSF information.
DEF_UTK_NETW	Char	8	2314	2321	The port of entry network name.
DEF_X500_SUBJECT	Char	255	2323	2577	Subject's name associated with this event.
DEF_X500_ISSUER	Char	255	2579	2833	Issuer's name associated with this event.

Event Qualifiers for DEFINE Resource Records

The event qualifiers that may be associated with a DEFINE event are shown in Table 17 on page 131.

Table 17. Event Qualifiers for Define Resource Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Successful definition.
UNDGROUP	01	Undefined group.
USNINGRP	02	User not in group.
INSAUTH	03	Insufficient authority.
ALRDEFD	04	Resource already defined.
NOTRACF	05	User is not RACF-defined.
NOTPROT	06	Resource not protected.
WNOTPROT	07	Warning: Resource not protected.
WSECLM	08	Warning: SECLABEL missing.
WINSSECL	09	Warning: insufficient SECLABEL.
NOT2RACF	10	User in second qualifier is not RACF-defined.
INSSECL	11	Insufficient SECLABEL authority.
LESSSPEC	12	A less-specific profile exists with a different SECLABEL.

The Format of the ADDSD Record Extension

Table 18 describes the format of a record that is created by the ADDSD command.

Table 18. Format of the ADDSD Record Extension (Event Code 08)

Field Name	Type	Length	Position		Comments
			Start	End	
AD_OWN_ID	Char	8	282	289	Owner of the profile.
AD_USER_NAME	Char	20	291	310	User name.
AD_SECL	Char	8	312	319	The SECLABEL associated with the profile.
AD_UTK_ENCR	Yes/No	4	321	324	Is the UTOKEN associated with this user encrypted?
AD_UTK_PRE19	Yes/No	4	326	329	Is this a pre-1.9 token?
AD_UTK_VERPROF	Yes/No	4	331	334	Is the VERIFYX propagation flag set?
AD_UTK_NJEUNUSR	Yes/No	4	336	339	Is this the NJE undefined user?
AD_UTK_LOGUSR	Yes/No	4	334	344	Is UAUDIT specified for this user?
AD_UTK_SPECIAL	Yes/No	4	346	349	Is this a SPECIAL user?
AD_UTK_DEFAULT	Yes/No	4	351	354	Is this a default token?
AD_UTK_UNKNUSR	Yes/No	4	356	359	Is this an undefined user?
AD_UTK_ERROR	Yes/No	4	361	364	Is this user token in error?
AD_UTK_TRUSTED	Yes/No	4	366	369	Is this user a part of the trusted computing base (TCB)?
AD_UTK_SESSTYPE	Char	8	371	378	The session type of this session.
AD_UTK_SURROGAT	Yes/No	4	380	383	Is this a surrogate user?
AD_UTK_REMOTE	Yes/No	4	385	388	Is this a remote job?
AD_UTK_PRIV	Yes/No	4	390	393	Is this a privileged user ID?
AD_UTK_SECL	Char	8	395	402	The SECLABEL of the user.
AD_UTK_EXECNODE	Char	8	404	411	The execution node of the work.
AD_UTK_SUSER_ID	Char	8	413	420	The submitting user ID.
AD_UTK_SNODE	Char	8	422	429	The submitting node.
AD_UTK_SGRP_ID	Char	8	431	438	The submitting group name.

SMF Data Unload—IRRADU00

Table 18. Format of the ADDSD Record Extension (Event Code 08) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
AD_UTK_SPOE	Char	8	440	447	The port of entry.
AD_UTK_SPCLASS	Char	8	449	456	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
AD_UTK_USER_ID	Char	8	458	465	User ID associated with the record.
AD_UTK_GRP_ID	Char	8	467	474	Group name associated with the record.
AD_UTK_DFT_GRP	Yes/No	4	476	479	Is a default group assigned?
AD_UTK_DFT_SECL	Yes/No	4	481	484	Is a default SECLABEL assigned?
AD_APPC_LINK	Char	16	486	501	Key to link together APPC records.
AD_SECL_LINK	Char	16	503	518	Key to link together the data sets affected by a change of SECLABEL and the command that caused the SECLABEL change.
AD_DS_NAME	Char	44	520	563	The data set name.
AD_SPECIFIED	Char	1024	565	1588	The keywords specified.
AD_FAILED	Char	1024	1590	2613	The keywords that failed.
AD_UTK_NETW	Char	8	2615	2622	The port of entry network name.
AD_X500_SUBJECT	Char	255	2624	2878	Subject's name associated with this event.
AD_X500_ISSUER	Char	255	2880	3134	Issuer's name associated with this event.

Event Qualifiers for ADDSD Commands

The event qualifiers that may be associated with an ADDSD command are shown in Table 19.

Table 19. Event Qualifiers for ADDSD Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.
KEYWVIOL	02	Keyword violation.
SECLSUCC	03	Successful retrieval of data set names.
SECLFAIL	04	Error during retrieval of data set names.

The Format of the ADDGROUP Record Extension

Table 20 describes the format of a record that is created by the ADDGROUP command.

Table 20. Format of the ADDGROUP Record Extension (Event Code 09)

Field Name	Type	Length	Position		Comments
			Start	End	
AG_OWN_ID	Char	8	282	289	Owner of the profile.
AG_USER_NAME	Char	20	291	310	User name.
AG_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
AG_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
AG_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
AG_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?

Table 20. Format of the ADDGROUP Record Extension (Event Code 09) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
AG_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
AG_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
AG_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
AG_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
AG_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
AG_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
AG_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
AG_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
AG_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
AG_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
AG_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
AG_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
AG_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
AG_UTK_SNODE	Char	8	413	420	The submitting node.
AG_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
AG_UTK_SPOE	Char	8	431	438	The port of entry.
AG_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
AG_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
AG_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
AG_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
AG_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
AG_APPC_LINK	Char	16	477	492	Key to link together APPC records.
AG_GRP_ID	Char	8	494	501	The group name.
AG_SPECIFIED	Char	1024	503	1526	The keywords specified.
AG_FAILED	Char	1024	1528	2551	The keywords that failed.
AG_UTK_NETW	Char	8	2553	2560	The port of entry network name.
AG_X500_SUBJECT	Char	255	2562	2816	Subject's name associated with this event.
AG_X500_ISSUER	Char	255	2818	3072	Issuer's name associated with this event.

Event Qualifiers for ADDGROUP Commands

The event qualifiers that may be associated with an ADDGROUP command are shown in Table 21.

Table 21. Event Qualifiers for ADDGROUP Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.
KEYWVIOL	02	Keyword violation.

SMF Data Unload—IRRADU00

The Format of the ADDUSER Record Extension

Table 22 describes the format of a record that is created by the ADDUSER command.

Table 22. Format of the ADDUSER Record Extension (Event Code 10)

Field Name	Type	Length	Position		Comments
			Start	End	
AU_OWN_ID	Char	8	282	289	Owner of the profile.
AU_USER_NAME	Char	20	291	310	User name.
AU_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
AU_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
AU_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
AU_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
AU_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
AU_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
AU_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
AU_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
AU_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
AU_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
AU_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
AU_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
AU_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
AU_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
AU_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
AU_UTK_EXECPNODE	Char	8	395	402	The execution node of the work.
AU_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
AU_UTK_SNODE	Char	8	413	420	The submitting node.
AU_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
AU_UTK_SPOE	Char	8	431	438	The port of entry.
AU_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
AU_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
AU_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
AU_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
AU_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
AU_APPC_LINK	Char	16	477	492	Key to link together APPC records.
AU_NOAUTH_CLAUTH	Yes/No	4	494	497	Were violations detected because the user issuing the command lacked the CLAUTH authority in the user class?
AU_NOAUTH_GROUP	Yes/No	4	499	502	Were violations detected because the user issuing the command lacked the authority within the group?
AU_USER_ID	Char	8	504	511	The user ID.
AU_SPECIFIED	Char	1024	513	1536	The keywords specified.
AU_FAILED	Char	1024	1538	2561	The keywords that failed.
AU_IGNORED	Char	1024	2563	3586	The keywords ignored.
AU_UTK_NETW	Char	8	3588	3595	The port of entry network name.
AU_X500_SUBJECT	Char	255	3597	3851	Subject's name associated with this event.

Table 22. Format of the ADDUSER Record Extension (Event Code 10) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
AU_X500_ISSUER	Char	255	3853	4107	Issuer's name associated with this event.

Event Qualifiers for ADDUSER Commands

The event qualifiers that may be associated with an ADDUSER command are shown in Table 23.

Table 23. Event Qualifiers for ADDUSER Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.
KEYWVIOL	02	Keyword violation.

The Format of the ALTDSD Record Extension

Table 24 describes the format of a record that is created by the ALTDSD command.

Table 24. Format of the ALTDSD Record Extension (Event Code 11)

Field Name	Type	Length	Position		Comments
			Start	End	
ALD_OWN_ID	Char	8	282	289	Owner of the profile.
ALD_USER_NAME	Char	20	291	310	User name.
ALD_OLD_SECL	Char	8	312	319	The SECLABEL that is being deleted from the profile.
ALD_UTK_ENCR	Yes/No	4	321	324	Is the UTOKEN associated with this user encrypted?
ALD_UTK_PRE19	Yes/No	4	326	329	Is this a pre-1.9 token?
ALD_UTK_VERPROF	Yes/No	4	331	334	Is the VERIFYX propagation flag set?
ALD_UTK_NJEUNUSR	Yes/No	4	336	339	Is this the NJE undefined user?
ALD_UTK_LOGUSR	Yes/No	4	341	344	Is UAUDIT specified for this user?
ALD_UTK_SPECIAL	Yes/No	4	346	349	Is this a SPECIAL user?
ALD_UTK_DEFAULT	Yes/No	4	351	354	Is this a default token?
ALD_UTK_UNKNUSR	Yes/No	4	356	359	Is this an undefined user?
ALD_UTK_ERROR	Yes/No	4	361	364	Is this user token in error?
ALD_UTK_TRUSTED	Yes/No	4	366	369	Is this user a part of the trusted computing base (TCB)?
ALD_UTK_SESSTYPE	Char	8	371	378	The session type of this session.
ALD_UTK_SURROGAT	Yes/No	4	380	383	Is this a surrogate user?
ALD_UTK_REMOTE	Yes/No	4	385	388	Is this a remote job?
ALD_UTK_PRIV	Yes/No	4	390	393	Is this a privileged user ID?
ALD_UTK_SECL	Char	8	395	402	The SECLABEL of the user.
ALD_UTK_EXECNODE	Char	8	404	411	The execution node of the work.
ALD_UTK_SUSER_ID	Char	8	413	420	The submitting user ID.
ALD_UTK_SNODE	Char	8	422	429	The submitting node.
ALD_UTK_SGRP_ID	Char	8	431	438	The submitting group name.
ALD_UTK_SPOE	Char	8	440	447	The port of entry.

SMF Data Unload—IRRADU00

Table 24. Format of the ALTDSD Record Extension (Event Code 11) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
ALD_UTK_SPCCLASS	Char	8	449	456	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
ALD_UTK_USER_ID	Char	8	458	465	User ID associated with the record.
ALD_UTK_GRP_ID	Char	8	467	474	Group name associated with the record.
ALD_UTK_DFT_GRP	Yes/No	4	476	479	Is a default group assigned?
ALD_UTK_DFT_SECL	Yes/No	4	481	484	Is a default SECLABEL assigned?
ALD_APPC_LINK	Char	16	486	501	Key to link together APPC records.
ALD_SECL_LINK	Char	16	503	518	Key to link together the data sets affected by a change of SECLABEL and the command that caused the SECLABEL change.
ALD_DS_NAME	Char	44	520	563	The data set name.
ALD_SPECIFIED	Char	1024	565	1588	The keywords specified.
ALD_FAILED	Char	1024	1590	2613	The keywords that failed.
ALD_IGNORED	Char	1024	2615	3638	The keywords ignored.
ALD_UTK_NETW	Char	8	3640	3647	The port of entry network name.
ALD_X500_SUBJECT	Char	255	3649	3903	Subject's name associated with this event.
ALD_X500_ISSUER	Char	255	3905	4159	Issuer's name associated with this event.

Event Qualifiers for ALTDSD Commands

The event qualifiers that may be associated with an ALTDSD command are shown in Table 25.

Table 25. Event Qualifiers for ADDSD Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.
KEYWVIOL	02	Keyword violation.
SECLSUCC	03	Successful retrieval of data set names.
SECLFAIL	04	Error during retrieval of data set names.

The Format of the ALTGROUP Record Extension

Table 26 describes the format of a record that is created by the ALTGROUP command.

Table 26. Format of the ALTGROUP Record Extension (Event Code 12)

Field Name	Type	Length	Position		Comments
			Start	End	
ALG_OWN_ID	Char	8	282	289	Owner of the profile.
ALG_USER_NAME	Char	20	291	310	User name.
ALG_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
ALG_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
ALG_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
ALG_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?

Table 26. Format of the ALTGROUP Record Extension (Event Code 12) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
ALG_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
ALG_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
ALG_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
ALG_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
ALG_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
ALG_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
ALG_UTK_SESTYPE	Char	8	362	369	The session type of this session.
ALG_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
ALG_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
ALG_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
ALG_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
ALG_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
ALG_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
ALG_UTK_SNODE	Char	8	413	420	The submitting node.
ALG_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
ALG_UTK_SPOE	Char	8	431	438	The port of entry.
ALG_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
ALG_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
ALG_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
ALG_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
ALG_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
ALG_APPC_LINK	Char	16	477	492	Key to link together APPC records.
ALG_GRP_ID	Char	8	494	501	The group name.
ALG_SPECIFIED	Char	1024	503	1526	The keywords specified.
ALG_FAILED	Char	1024	1528	2551	The keywords that failed.
ALG_IGNORED	Char	1024	2553	3576	The keywords ignored.
ALG_UTK_NETW	Char	8	3578	3585	The port of entry network name.
ALG_X500_SUBJECT	Char	255	3587	3841	Subject's name associated with this event.
ALG_X500_ISSUER	Char	255	3843	4097	Issuer's name associated with this event.

Event Qualifiers for ALTGROUP Commands

The event qualifiers that may be associated with an ALTGROUP command are shown in Table 27.

Table 27. Event Qualifiers for ALTGROUP Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.
KEYWVIOL	02	Keyword violation.

SMF Data Unload—IRRADU00

The Format of the ALTUSER Record Extension

Table 28 describes the format of a record that is created by the ALTUSER command.

Table 28. Format of the ALTUSER Record Extension (Event Code 13)

Field Name	Type	Length	Position		Comments
			Start	End	
ALU_OWN_ID	Char	8	282	289	Owner of the profile.
ALU_USER_NAME	Char	20	291	310	User name.
ALU_OLD_SECL	Char	8	312	319	The SECLABEL that is being deleted from the profile.
ALU_UTK_ENCR	Yes/No	4	321	324	Is the UTOKEN associated with this user encrypted?
ALU_UTK_PRE19	Yes/No	4	326	329	Is this a pre-1.9 token?
ALU_UTK_VERPROF	Yes/No	4	331	334	Is the VERIFYX propagation flag set?
ALU_UTK_NJEUNUSR	Yes/No	4	336	339	Is this the NJE undefined user?
ALU_UTK_LOGUSR	Yes/No	4	341	344	Is UAUDIT specified for this user?
ALU_UTK_SPECIAL	Yes/No	4	346	349	Is this a SPECIAL user?
ALU_UTK_DEFAULT	Yes/No	4	351	354	Is this a default token?
ALU_UTK_UNKNUSR	Yes/No	4	356	359	Is this an undefined user?
ALU_UTK_ERROR	Yes/No	4	361	364	Is this user token in error?
ALU_UTK_TRUSTED	Yes/No	4	366	369	Is this user a part of the trusted computing base (TCB)?
ALU_UTK_SESSTYPE	Char	8	371	378	The session type of this session.
ALU_UTK_SURROGAT	Yes/No	4	380	383	Is this a surrogate user?
ALU_UTK_REMOTE	Yes/No	4	385	388	Is this a remote job?
ALU_UTK_PRIV	Yes/No	4	390	393	Is this a privileged user ID?
ALU_UTK_SECL	Char	8	395	402	The SECLABEL of the user.
ALU_UTK_EXECNODE	Char	8	404	411	The execution node of the work.
ALU_UTK_SUSER_ID	Char	8	4413	420	The submitting user ID.
ALU_UTK_SNODE	Char	8	422	429	The submitting node.
ALU_UTK_SGRP_ID	Char	8	431	438	The submitting group name.
ALU_UTK_SPOE	Char	8	440	447	The port of entry.
ALU_UTK_SPCLASS	Char	8	449	456	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
ALU_UTK_USER_ID	Char	8	458	465	User ID associated with the record.
ALU_UTK_GRP_ID	Char	8	467	474	Group name associated with the record.
ALU_UTK_DFT_GRP	Yes/No	4	476	479	Is a default group assigned?
ALU_UTK_DFT_SECL	Yes/No	4	481	484	Is a default SECLABEL assigned?
ALU_APPC_LINK	Char	16	486	501	Key to link together APPC records.
ALU_NOAUTH_CLAUTH	Yes/No	4	503	506	Were violations detected because the user issuing the command lacked the CLAUTH authority in the user class?
ALU_NOAUTH_GROUP	Yes/No	4	508	511	Were violations detected because the user issuing the command lacked the authority within the group?
ALU_NOAUTH_PROF	Yes/No	4	513	516	Were violations detected because the user issuing the command lacked authority to the profile?
ALU_USER_ID	Char	8	518	525	The user ID.
ALU_SPECIFIED	Char	1024	527	1550	The keywords specified.

Table 28. Format of the ALTUSER Record Extension (Event Code 13) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
ALU_FAILED	Char	1024	1552	2575	The keywords that failed.
ALU_IGNORED	Char	1024	2577	3600	The keywords ignored.
ALU_UTK_NETW	Char	8	3602	3609	The port of entry network name.
ALU_X500_SUBJECT	Char	255	3611	3865	Subject's name associated with this event.
ALU_X500_ISSUER	Char	255	3867	4121	Issuer's name associated with this event.

Event Qualifiers for ALTUSER Commands

The event qualifiers that may be associated with an ALTUSER command are shown in Table 29.

Table 29. Event Qualifiers for ALTUSER Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.
KEYWVIOL	02	Keyword violation.

The Format of the CONNECT Record Extension

Table 30 describes the format of a record that is created by the CONNECT command.

Table 30. Format of the CONNECT Record Extension (Event Code 14)

Field Name	Type	Length	Position		Comments
			Start	End	
CON_OWN_ID	Char	8	282	289	Owner of the profile.
CON_USER_NAME	Char	20	291	310	User name.
CON_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
CON_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
CON_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
CON_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
CON_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
CON_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
CON_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
CON_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
CON_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
CON_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
CON_UTK_SESTYPE	Char	8	362	369	The session type of this session.
CON_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
CON_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
CON_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
CON_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
CON_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
CON_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.

SMF Data Unload—IRRADU00

Table 30. Format of the CONNECT Record Extension (Event Code 14) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
CON_UTK_SNODE	Char	8	413	420	The submitting node.
CON_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
CON_UTK_SPOE	Char	8	431	438	The port of entry.
CON_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
CON_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
CON_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
CON_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
CON_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
CON_APPC_LINK	Char	16	477	492	Key to link together APPC records.
CON_USER_ID	Char	8	494	501	The user ID that is being connected.
CON_SPECIFIED	Char	1024	503	1526	The keywords specified.
CON_FAILED	Char	1024	1528	2551	The keywords ignored.
CON_UTK_NETW	Char	8	2553	2560	The port of entry network name.
CON_X500_SUBJECT	Char	255	2562	2816	Subject's name associated with this event.
CON_X500_ISSUER	Char	255	2818	3072	Issuer's name associated with this event.

Event Qualifiers for CONNECT Commands

The event qualifiers that may be associated with an CONNECT command are shown in Table 31.

Table 31. Event Qualifiers for CONNECT Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.
KEYWVIOL	02	Keyword violation.

The Format of the DELDSD Record Extension

Table 32 describes the format of a record that is created by the DELDSD command.

Table 32. Format of the DELDSD Record Extension (Event Code 15)

Field Name	Type	Length	Position		Comments
			Start	End	
DELD_OWN_ID	Char	8	282	289	Owner of the profile.
DELD_USER_NAME	Char	20	291	310	User name.
DELD_OLD_SECL	Char	8	312	319	The SECLABEL that is being deleted.
DELD_UTK_ENCR	Yes/No	4	321	324	Is the UTOKEN associated with this user encrypted?
DELD_UTK_PRE19	Yes/No	4	326	329	Is this a pre-1.9 token?
DELD_UTK_VERPROF	Yes/No	4	331	334	Is the VERIFYX propagation flag set?
DELD_UTK_NJEUNUSR	Yes/No	4	336	339	Is this the NJE undefined user?
DELD_UTK_LOGUSR	Yes/No	4	341	344	Is UAUDIT specified for this user?
DELD_UTK_SPECIAL	Yes/No	4	346	349	Is this a SPECIAL user?

Table 32. Format of the DELDSD Record Extension (Event Code 15) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
DELD_UTK_DEFAULT	Yes/No	4	351	354	Is this a default token?
DELD_UTK_UNKNUSR	Yes/No	4	356	359	Is this an undefined user?
DELD_UTK_ERROR	Yes/No	4	361	364	Is this user token in error?
DELD_UTK_TRUSTED	Yes/No	4	366	369	Is this user a part of the trusted computing base (TCB)?
DELD_UTK_SESSTYPE	Char	8	371	378	The session type of this session.
DELD_UTK_SURROGAT	Yes/No	4	380	383	Is this a surrogate user?
DELD_UTK_REMOTE	Yes/No	4	385	388	Is this a remote job?
DELD_UTK_PRIV	Yes/No	4	390	393	Is this a privileged user ID?
DELD_UTK_SECL	Char	8	395	402	The SECLABEL of the user.
DELD_UTK_EXECNODE	Char	8	404	411	The execution node of the work.
DELD_UTK_SUSER_ID	Char	8	413	420	The submitting user ID.
DELD_UTK_SNODE	Char	8	422	429	The submitting node.
DELD_UTK_SGRP_ID	Char	8	431	438	The submitting group name.
DELD_UTK_SPOE	Char	8	440	447	The port of entry.
DELD_UTK_SPCCLASS	Char	8	449	456	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
DELD_UTK_USER_ID	Char	8	458	465	User ID associated with the record.
DELD_UTK_GRP_ID	Char	8	467	474	Group name associated with the record.
DELD_UTK_DFT_GRP	Yes/No	4	476	479	Is a default group assigned?
DELD_UTK_DFT_SECL	Yes/No	4	481	484	Is a default SECLABEL assigned?
DELD_APPC_LINK	Char	16	486	501	Key to link together APPC records.
DELD_SECL_LINK	Char	16	503	518	Key to link together the data sets affected by a change of SECLABEL and the command that caused the SECLABEL change.
DELD_DS_NAME	Char	44	520	563	The data set profile that is being deleted.
DELD_SPECIFIED	Char	1024	565	1588	The keywords specified.
DELD_FAILED	Char	1024	1590	2613	The keywords that failed.
DELD_UTK_NETW	Char	8	2615	2622	The port of entry network name.
DELD_X500_SUBJECT	Char	255	2624	2878	Subject's name associated with this event.
DELD_X500_ISSUER	Char	255	2880	3134	Issuer's name associated with this event.

Event Qualifiers for DELDSD Commands

The event qualifiers that may be associated with an DELDSD command are shown in Table 33.

Table 33. Event Qualifiers for DELDSD Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.
KEYWVIOL	02	Keyword violation.
SECLSUCC	03	Successful retrieval of data set names.
SECLFAIL	04	Error during retrieval of data set names.

SMF Data Unload—IRRADU00

The Format of the DELGROUP Record Extension

Table 34 describes the format of a record that is created by the DELGROUP command.

Table 34. Format of the DELGROUP Record Extension (Event Code 16)

Field Name	Type	Length	Position		Comments
			Start	End	
DELG_OWN_ID	Char	8	282	289	Owner of the profile.
DELG_USER_NAME	Char	20	291	310	User name.
DELG_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
DELG_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
DELG_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
DELG_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
DELG_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
DELG_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
DELG_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
DELG_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
DELG_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
DELG_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
DELG_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
DELG_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
DELG_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
DELG_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
DELG_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
DELG_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
DELG_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
DELG_UTK_SNODE	Char	8	413	420	The submitting node.
DELG_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
DELG_UTK_SPOE	Char	8	431	438	The port of entry.
DELG_UTK_SPCCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
DELG_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
DELG_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
DELG_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
DELG_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
DELG_APPC_LINK	Char	16	477	492	Key to link together APPC records.
DELG_GRP_ID	Char	8	494	501	The group that is being deleted.
DELG_SPECIFIED	Char	1024	503	1526	The RRSF keywords specified.
DELG_UTK_NETW	Char	8	1528	1535	The port of entry network name.
DELG_X500_SUBJECT	Char	255	1537	1791	Subject's name associated with this event.
DELG_X500_ISSUER	Char	255	1793	2047	Issuer's name associated with this event.

Event Qualifiers for DELGROUP Commands

The event qualifiers that may be associated with an DELGROUP command are shown in Table 35 on page 143.

Table 35. Event Qualifiers for DELGROUP Commands Records.

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.
KEYWVIOL	02	Keyword violation.

The Format of the DELUSER Record Extension

Table 36 describes the format of a record that is created by the DELUSER command.

Table 36. Format of the DELUSER Record Extension (Event Code 17)

Field Name	Type	Length	Position		Comments
			Start	End	
DELU_OWN_ID	Char	8	282	289	Owner of the profile.
DELU_USER_NAME	Char	20	291	310	User name.
DELU_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
DELU_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
DELU_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
DELU_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
DELU_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
DELU_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
DELU_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
DELU_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
DELU_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
DELU_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
DELU_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
DELU_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
DELU_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
DELU_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
DELU_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
DELU_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
DELU_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
DELU_UTK_SNODE	Char	8	413	420	The submitting node.
DELU_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
DELU_UTK_SPOE	Char	8	431	438	The port of entry.
DELU_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
DELU_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
DELU_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
DELU_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
DELU_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
DELU_APPC_LINK	Char	16	477	492	Key to link together APPC records.
DELU_USER_ID	Char	8	494	501	The user ID that is being deleted.
DELU_SPECIFIED	Char	1024	503	1526	The RRSF keywords specified.
DELU_UTK_NETW	Char	8	1528	1535	The port of entry network name.

SMF Data Unload—IRRADU00

Table 36. Format of the DELUSER Record Extension (Event Code 17) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
DELU_X500_SUBJECT	Char	255	1537	1791	Subject's name associated with this event.
DELU_X500_ISSUER	Char	255	1793	2047	Issuer's name associated with this event.

Event Qualifiers for DELUSER Commands

The event qualifiers that may be associated with a DELUSER command are shown in Table 37.

Table 37. Event Qualifiers for DELUSER Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.
KEYWVIOL	02	Keyword violation.

The Format of the PASSWORD Record Extension

Table 38 describes the format of a record that is created by the PASSWORD command.

Table 38. Format of the PASSWORD Record Extension (Event Code 18)

Field Name	Type	Length	Position		Comments
			Start	End	
PWD_OWN_ID	Char	8	282	289	Owner of the profile.
PWD_USER_NAME	Char	20	291	310	User name.
PWD_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
PWD_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
PWD_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
PWD_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
PWD_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
PWD_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
PWD_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
PWD_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
PWD_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
PWD_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
PWD_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
PWD_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
PWD_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
PWD_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
PWD_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
PWD_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
PWD_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
PWD_UTK_SNODE	Char	8	413	420	The submitting node.
PWD_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
PWD_UTK_SPOE	Char	8	431	438	The port of entry.

Table 38. Format of the PASSWORD Record Extension (Event Code 18) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
PWD_UTK_SPCCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
PWD_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
PWD_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
PWD_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
PWD_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
PWD_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
PWD_SPECIFIED	Char	1024	494	1517	The keywords specified.
PWD_FAILED	Char	1024	1519	2542	The keywords that failed.
PWD_IGNORED	Char	1024	2544	3567	The keywords ignored.
PWD_UTK_NETW	Char	8	3569	3576	The port of entry network name.
PWD_X500_SUBJECT	Char	255	3578	3832	Subject's name associated with this event.
PWD_X500_ISSUER	Char	255	3834	4088	Issuer's name associated with this event.

Event Qualifiers for PASSWORD Commands

The event qualifiers that may be associated with a PASSWORD command are shown in Table 39.

Table 39. Event Qualifiers for PASSWORD Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.
KEYWVIOL	02	Keyword violation.

The Format of the PERMIT Record Extension

Table 40 describes the format of a record that is created by the PERMIT command.

Table 40. Format of the PERMIT Record Extension (Event Code 19)

Field Name	Type	Length	Position		Comments
			Start	End	
PERM_CLASS	Char	8	282	289	Class name.
PERM_OWN_ID	Char	8	291	298	Owner of the profile.
PERM_USER_NAME	Char	20	300	319	User name.
PERM_UTK_ENCR	Yes/No	4	321	324	Is the UTOKEN associated with this user encrypted?
PERM_UTK_PRE19	Yes/No	4	326	329	Is this a pre-1.9 token?
PERM_UTK_VERPROF	Yes/No	4	331	334	Is the VERIFYX propagation flag set?
PERM_UTK_NJEUNUSR	Yes/No	4	336	339	Is this the NJE undefined user?
PERM_UTK_LOGUSR	Yes/No	4	341	344	Is UAUDIT specified for this user?
PERM_UTK_SPECIAL	Yes/No	4	346	349	Is this a SPECIAL user?
PERM_UTK_DEFAULT	Yes/No	4	351	354	Is this a default token?
PERM_UTK_UNKNUSR	Yes/No	4	356	359	Is this an undefined user?

SMF Data Unload—IRRADU00

Table 40. Format of the PERMIT Record Extension (Event Code 19) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
PERM_UTK_ERROR	Yes/No	4	361	364	Is this user token in error?
PERM_UTK_TRUSTED	Yes/No	4	366	369	Is this user a part of the trusted computing base (TCB)?
PERM_UTK_SESTYPE	Char	8	371	378	The session type of this session.
PERM_UTK_SURROGAT	Yes/No	4	380	383	Is this a surrogate user?
PERM_UTK_REMOTE	Yes/No	4	385	388	Is this a remote job?
PERM_UTK_PRIV	Yes/No	4	390	393	Is this a privileged user ID?
PERM_UTK_SECL	Char	8	395	402	The SECLABEL of the user.
PERM_UTK_EXECNODE	Char	8	404	411	The execution node of the work.
PERM_UTK_SUSER_ID	Char	8	413	420	The submitting user ID.
PERM_UTK_SNODE	Char	8	422	429	The submitting node.
PERM_UTK_SGRP_ID	Char	8	431	438	The submitting group name.
PERM_UTK_SPOE	Char	8	440	447	The port of entry.
PERM_UTK_SPCLASS	Char	8	449	456	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
PERM_UTK_USER_ID	Char	8	458	465	User ID associated with the record.
PERM_UTK_GRP_ID	Char	8	467	474	Group name associated with the record.
PERM_UTK_DFT_GRP	Yes/No	4	476	479	Is a default group assigned?
PERM_UTK_DFT_SECL	Yes/No	4	481	484	Is a default SECLABEL assigned?
PERM_APPC_LINK	Char	16	486	501	Key to link together APPC records.
PERM_RES_NAME	Char	255	503	757	The resource name
PERM_SPECIFIED	Char	1024	759	1782	The keywords specified.
PERM_FAILED	Char	1024	1784	2807	The keywords that failed.
PERM_IGNORED	Char	1024	2809	3832	The keywords ignored.
PERM_UTK_NETW	Char	8	3834	3841	The port of entry network name.
PERM_X500_SUBJECT	Char	255	3843	4097	Subject's name associated with this event.
PERM_X500_ISSUER	Char	255	4099	4353	Issuer's name associated with this event.

Event Qualifiers for PERMIT Commands

The event qualifiers that may be associated with a PERMIT command are shown in Table 41.

Table 41. Event Qualifiers for PERMIT Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.
KEYWVIOL	02	Keyword violation.

The Format of the RALTER Record Extension

Table 42 on page 147 describes the format of a record that is created by the RALTER command.

Table 42. Format of the RALTER Record Extension (Event Code 20)

Field Name	Type	Length	Position		Comments
			Start	End	
RALT_CLASS	Char	8	282	289	Class name.
RALT_OWN_ID	Char	8	291	298	Owner of the profile.
RALT_USER_NAME	Char	20	300	319	User name.
RALT_OLD_SECL	Char	8	321	328	The SECLABEL being deleted from the file.
RALT_UTK_ENCR	Yes/No	4	330	333	Is the UTOKEN associated with this user encrypted?
RALT_UTK_PRE19	Yes/No	4	335	338	Is this a pre-1.9 token?
RALT_UTK_VERPROF	Yes/No	4	340	343	Is the VERIFYX propagation flag set?
RALT_UTK_NJEUNUSR	Yes/No	4	345	348	Is this the NJE undefined user?
RALT_UTK_LOGUSR	Yes/No	4	350	353	Is UAUDIT specified for this user?
RALT_UTK_SPECIAL	Yes/No	4	355	358	Is this a SPECIAL user?
RALT_UTK_DEFAULT	Yes/No	4	360	363	Is this a default token?
RALT_UTK_UNKNUSR	Yes/No	4	365	368	Is this an undefined user?
RALT_UTK_ERROR	Yes/No	4	370	373	Is this user token in error?
RALT_UTK_TRUSTED	Yes/No	4	375	378	Is this user a part of the trusted computing base (TCB)?
RALT_UTK_SESSTYPE	Char	8	380	387	The session type of this session.
RALT_UTK_SURROGAT	Yes/No	4	389	392	Is this a surrogate user?
RALT_UTK_REMOTE	Yes/No	4	394	397	Is this a remote job?
RALT_UTK_PRIV	Yes/No	4	399	402	Is this a privileged user ID?
RALT_UTK_SECL	Char	8	404	411	The SECLABEL of the user.
RALT_UTK_EXECNODE	Char	8	413	420	The execution node of the work.
RALT_UTK_SUSER_ID	Char	8	422	429	The submitting user ID.
RALT_UTK_SNODE	Char	8	431	438	The submitting node.
RALT_UTK_SGRP_ID	Char	8	440	447	The submitting group name.
RALT_UTK_SPOE	Char	8	449	456	The port of entry.
RALT_UTK_SPCLASS	Char	8	458	465	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
RALT_UTK_USER_ID	Char	8	467	474	User ID associated with the record.
RALT_UTK_GRP_ID	Char	8	476	483	Group name associated with the record.
RALT_UTK_DFT_GRP	Yes/No	4	485	488	Is a default group assigned?
RALT_UTK_DFT_SECL	Yes/No	4	490	493	Is a default SECLABEL assigned?
RALT_APPC_LINK	Char	16	495	510	Key to link together APPC records.
RALT_RES_NAME	Char	255	512	766	The resource name.
RALT_SPECIFIED	Char	1024	768	1791	The keywords specified.
RALT_FAILED	Char	1024	1793	2816	The keywords that failed.
RALT_UTK_NETW	Char	8	2818	2825	The port of entry network name.
RALT_X500_SUBJECT	Char	255	2827	3081	Subject's name associated with this event.
RALT_X500_ISSUER	Char	255	3083	3337	Issuer's name associated with this event.

Event Qualifiers for RALTER Commands

The event qualifiers that may be associated with a RALTER command are shown in Table 43 on page 148.

SMF Data Unload—IRRADU00

Table 43. Event Qualifiers for RALTER Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.
KEYWVIOL	02	Keyword violation.

The Format of the RDEFINE Record Extension

Table 44 describes the format of a record that is created by the RDEFINE command.

Table 44. Format of the RDEFINE Record Extension (Event Code 21)

Field Name	Type	Length	Position		Comments
			Start	End	
RDEF_CLASS	Char	8	282	289	Class name.
RDEF_OWN_ID	Char	8	291	298	Owner of the profile.
RDEF_USER_NAME	Char	20	300	319	User name.
RDEF_SECL	Char	8	321	328	The SECLABEL associated with the profile.
RDEF_UTK_ENCR	Yes/No	4	330	333	Is the UTOKEN associated with this user encrypted?
RDEF_UTK_PRE19	Yes/No	4	335	338	Is this a pre-1.9 token?
RDEF_UTK_VERPROF	Yes/No	4	340	343	Is the VERIFYX propagation flag set?
RDEF_UTK_NJEUNUSR	Yes/No	4	345	348	Is this the NJE undefined user?
RDEF_UTK_LOGUSR	Yes/No	4	350	353	Is UAUDIT specified for this user?
RDEF_UTK_SPECIAL	Yes/No	4	355	358	Is this a SPECIAL user?
RDEF_UTK_DEFAULT	Yes/No	4	360	363	Is this a default token?
RDEF_UTK_UNKNUSR	Yes/No	4	365	368	Is this an undefined user?
RDEF_UTK_ERROR	Yes/No	4	370	373	Is this user token in error?
RDEF_UTK_TRUSTED	Yes/No	4	375	378	Is this user a part of the trusted computing base (TCB)?
RDEF_UTK_SESSTYPE	Char	8	380	387	The session type of this session.
RDEF_UTK_SURROGAT	Yes/No	4	389	392	Is this a surrogate user?
RDEF_UTK_REMOTE	Yes/No	4	394	397	Is this a remote job?
RDEF_UTK_PRIV	Yes/No	4	399	402	Is this a privileged user ID?
RDEF_UTK_SECL	Char	8	404	411	The SECLABEL of the user.
RDEF_UTK_EXECNODE	Char	8	413	420	The execution node of the work.
RDEF_UTK_SUSER_ID	Char	8	422	429	The submitting user ID.
RDEF_UTK_SNODE	Char	8	431	438	The submitting node.
RDEF_UTK_SGRP_ID	Char	8	440	447	The submitting group name.
RDEF_UTK_SPOE	Char	8	449	456	The port of entry.
RDEF_UTK_SPCCLASS	Char	8	458	465	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
RDEF_UTK_USER_ID	Char	8	467	474	User ID associated with the record.
RDEF_UTK_GRP_ID	Char	8	476	483	Group name associated with the record.
RDEF_UTK_DFT_GRP	Yes/No	4	485	488	Is a default group assigned?
RDEF_UTK_DFT_SECL	Yes/No	4	490	493	Is a default SECLABEL assigned?
RDEF_APPC_LINK	Char	16	495	510	Key to link together APPC records.
RDEF_RES_NAME	Char	255	512	766	The resource name.

Table 44. Format of the RDEFINE Record Extension (Event Code 21) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
RDEF_SPECIFIED	Char	1024	768	1791	The keywords specified.
RDEF_FAILED	Char	1024	1793	2816	The keywords that failed.
RDEF_UTK_NETW	Char	8	2818	2825	The port of entry network name.
RDEF_X500_SUBJECT	Char	255	2827	3081	Subject's name associated with this event.
RDEF_X500_ISSUER	Char	255	3083	3337	Issuer's name associated with this event.

Event Qualifiers for RDEFINE Commands

The event qualifiers that may be associated with a RDEFINE command are shown in Table 45.

Table 45. Event Qualifiers for RDEFINE Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.
KEYWVIOL	02	Keyword violation.

The Format of the RDELETE Record Extension

Table 46 describes the format of a record that is created by the RDELETE command.

Table 46. Format of the RDELETE Record Extension (Event Code 22)

Field Name	Type	Length	Position		Comments
			Start	End	
RDEL_CLASS	Char	8	282	289	Class name.
RDEL_OWN_ID	Char	8	291	298	Owner of the profile.
RDEL_USER_NAME	Char	20	300	319	User name.
RDEL_SECL	Char	8	321	328	The SECLABEL associated with the profile.
RDEL_UTK_ENCR	Yes/No	4	330	333	Is the UTOKEN associated with this user encrypted?
RDEL_UTK_PRE19	Yes/No	4	335	338	Is this a pre-1.9 token?
RDEL_UTK_VERPROF	Yes/No	4	340	343	Is the VERIFYX propagation flag set?
RDEL_UTK_NJEUNUSR	Yes/No	4	345	348	Is this the NJE undefined user?
RDEL_UTK_LOGUSR	Yes/No	4	350	353	Is UAUDIT specified for this user?
RDEL_UTK_SPECIAL	Yes/No	4	355	358	Is this a SPECIAL user?
RDEL_UTK_DEFAULT	Yes/No	4	360	363	Is this a default token?
RDEL_UTK_UNKNUSR	Yes/No	4	365	368	Is this an undefined user?
RDEL_UTK_ERROR	Yes/No	4	370	373	Is this user token in error?
RDEL_UTK_TRUSTED	Yes/No	4	375	378	Is this user a part of the trusted computing base (TCB)?
RDEL_UTK_SESSTYPE	Char	8	380	387	The session type of this session.
RDEL_UTK_SURROGAT	Yes/No	4	389	392	Is this a surrogate user?
RDEL_UTK_REMOTE	Yes/No	4	394	397	Is this a remote job?
RDEL_UTK_PRIV	Yes/No	4	399	402	Is this a privileged user ID?
RDEL_UTK_SECL	Char	8	404	411	The SECLABEL of the user.

SMF Data Unload—IRRADU00

Table 46. Format of the RDELETE Record Extension (Event Code 22) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
RDEL_UTK_EXECNODE	Char	8	413	420	The execution node of the work.
RDEL_UTK_SUSER_ID	Char	8	422	429	The submitting user ID.
RDEL_UTK_SNODE	Char	8	431	438	The submitting node.
RDEL_UTK_SGRP_ID	Char	8	440	447	The submitting group name.
RDEL_UTK_SPOE	Char	8	449	456	The port of entry.
RDEL_UTK_SPCLASS	Char	8	458	465	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
RDEL_UTK_USER_ID	Char	8	467	474	User ID associated with the record.
RDEL_UTK_GRP_ID	Char	8	476	483	Group name associated with the record.
RDEL_UTK_DFT_GRP	Yes/No	4	485	488	Is a default group assigned?
RDEL_UTK_DFT_SECL	Yes/No	4	490	493	Is a default SECLABEL assigned?
RDEL_APPC_LINK	Char	16	495	510	Key to link together APPC records.
RDEL_RES_NAME	Char	255	512	766	The resource name.
RDEL_SPECIFIED	Char	1024	768	1791	The keywords specified.
RDEL_UTK_NETW	Char	8	1793	1800	The port of entry network name.
RDEL_X500_SUBJECT	Char	255	1802	2056	Subject's name associated with this event.
RDEL_X500_ISSUER	Char	255	2058	2312	Issuer's name associated with this event.

Event Qualifiers for RDELETE Commands

The event qualifiers that may be associated with a RDELETE command are shown in Table 47.

Table 47. Event Qualifiers for RDELETE Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.
KEYWVIOL	02	Keyword violation.

The Format of the REMOVE Record Extension

Table 48 describes the format of a record that is created by the REMOVE command.

Table 48. Format of the REMOVE Record Extension (Event Code 23)

Field Name	Type	Length	Position		Comments
			Start	End	
REM_OWN_ID	Char	8	282	289	Owner of the profile.
REM_USER_NAME	Char	20	291	310	User name.
REM_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
REM_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
REM_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
REM_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
REM_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
REM_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?

Table 48. Format of the REMOVE Record Extension (Event Code 23) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
REM_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
REM_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
REM_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
REM_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
REM_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
REM_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
REM_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
REM_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
REM_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
REM_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
REM_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
REM_UTK_SNODE	Char	8	413	420	The submitting node.
REM_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
REM_UTK_SPOE	Char	8	431	438	The port of entry.
REM_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
REM_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
REM_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
REM_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
REM_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
REM_APPC_LINK	Char	16	477	492	Key to link together APPC records.
REM_USER_ID	Char	8	494	501	The user ID.
REM_SPECIFIED	Char	1024	503	1526	The keywords specified.
REM_FAILED	Char	1024	1528	2551	The keywords that failed.
REM_UTK_NETW	Char	8	2553	2560	The port of entry network name.
REM_X500_SUBJECT	Char	255	2562	2816	Subject's name associated with this event.
REM_X500_ISSUER	Char	255	2818	3072	Issuer's name associated with this event.

Event Qualifiers for REMOVE Commands

The event qualifiers that may be associated with a REMOVE command are shown in Table 49.

Table 49. Event Qualifiers for REMOVE Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.
KEYWVIOL	02	Keyword violation.

The Format of the SETROPTS Record Extension

Table 50 on page 152 describes record format that is created by the SETROPTS command.

SMF Data Unload—IRRADU00

Table 50. Format of the SETROPTS Record Extension (Event Code 24)

Field Name	Type	Length	Position		Comments
			Start	End	
SETR_USER_NAME	Char	20	282	301	User name.
SETR_UTK_ENCR	Yes/No	4	303	306	Is the UTOKEN associated with this user encrypted?
SETR_UTK_PRE19	Yes/No	4	308	311	Is this a pre-1.9 token?
SETR_UTK_VERPROF	Yes/No	4	313	316	Is the VERIFYX propagation flag set?
SETR_UTK_NJEUNUSR	Yes/No	4	318	321	Is this the NJE undefined user?
SETR_UTK_LOGUSR	Yes/No	4	323	326	Is UAUDIT specified for this user?
SETR_UTK_SPECIAL	Yes/No	4	328	331	Is this a SPECIAL user?
SETR_UTK_DEFAULT	Yes/No	4	333	336	Is this a default token?
SETR_UTK_UNKNUSR	Yes/No	4	338	341	Is this an undefined user?
SETR_UTK_ERROR	Yes/No	4	343	346	Is this user token in error?
SETR_UTK_TRUSTED	Yes/No	4	348	351	Is this user a part of the trusted computing base (TCB)?
SETR_UTK_SESSTYPE	Char	8	353	360	The session type of this session.
SETR_UTK_SURROGAT	Yes/No	4	362	365	Is this a surrogate user?
SETR_UTK_REMOVE	Yes/No	4	367	370	Is this a remote job?
SETR_UTK_PRIV	Yes/No	4	372	375	Is this a privileged user ID?
SETR_UTK_SECL	Char	8	377	384	The SECLABEL of the user.
SETR_UTK_EXECNODE	Char	8	386	393	The execution node of the work.
SETR_UTK_SUSER_ID	Char	8	395	402	The submitting user ID.
SETR_UTK_SNODE	Char	8	404	411	The submitting node.
SETR_UTK_SGRP_ID	Char	8	413	420	The submitting group name.
SETR_UTK_SPOE	Char	8	422	429	The port of entry.
SETR_UTK_SPCCLASS	Char	8	431	438	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
SETR_UTK_USER_ID	Char	8	440	447	User ID associated with the record.
SETR_UTK_GRP_ID	Char	8	449	456	Group name associated with the record.
SETR_UTK_DFT_GRP	Yes/No	4	458	461	Is a default group assigned?
SETR_UTK_DFT_SECL	Yes/No	4	463	466	Is a default SECLABEL assigned?
SETR_APPC_LINK	Char	16	468	483	Key to link together APPC records.
SETR_SPECIFIED	Char	1024	485	1508	The keywords specified.
SETR_FAILED	Char	1024	1510	2533	The keywords that failed.
SETR_UTK_NETW	Char	8	2535	2542	The port of entry network name.
SETR_X500_SUBJECT	Char	255	2544	2798	Subject's name associated with this event.
SETR_X500_ISSUER	Char	255	2800	3054	Issuer's name associated with this event.

Event Qualifiers for SETROPTS Commands

Table 51 shows event qualifiers associated with a SETROPTS command.

Table 51. Event Qualifiers for SETROPTS Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.

Table 51. Event Qualifiers for SETROPTS Command Records (continued)

Event Qualifier	Event Qualifier Number	Event Description
KEYWVIOL	02	Keyword violation.

The Format of the RVAR_Y Record Extension

Table 52 describes the format of a record that is created by the RVAR_Y command.

Table 52. Format of the RVAR_Y Record Extension (Event Code 25)

Field Name	Type	Length	Position		Comments
			Start	End	
RVAR_USER_NAME	Char	20	282	301	User name.
RVAR_UTK_ENCR	Yes/No	4	303	306	Is the UTOKEN associated with this user encrypted?
RVAR_UTK_PRE19	Yes/No	4	308	311	Is this a pre-1.9 token?
RVAR_UTK_VERPROF	Yes/No	4	313	316	Is the VERIFYX propagation flag set?
RVAR_UTK_NJEUNUSR	Yes/No	4	318	321	Is this the NJE undefined user?
RVAR_UTK_LOGUSR	Yes/No	4	323	326	Is UAUDIT specified for this user?
RVAR_UTK_SPECIAL	Yes/No	4	328	331	Is this a SPECIAL user?
RVAR_UTK_DEFAULT	Yes/No	4	333	336	Is this a default token?
RVAR_UTK_UNKNUSR	Yes/No	4	338	341	Is this an undefined user?
RVAR_UTK_ERROR	Yes/No	4	343	346	Is this user token in error?
RVAR_UTK_TRUSTED	Yes/No	4	348	351	Is this user a part of the trusted computing base (TCB)?
RVAR_UTK_SESSTYPE	Char	8	353	360	The session type of this session.
RVAR_UTK_SURROGAT	Yes/No	4	362	365	Is this a surrogate user?
RVAR_UTK_REMOTE	Yes/No	4	367	370	Is this a remote job?
RVAR_UTK_PRIV	Yes/No	4	372	375	Is this a privileged user ID?
RVAR_UTK_SECL	Char	8	377	384	The SECLABEL of the user.
RVAR_UTK_EXECNODE	Char	8	386	393	The execution node of the work.
RVAR_UTK_SUSER_ID	Char	8	395	402	The submitting user ID.
RVAR_UTK_SNODE	Char	8	404	411	The submitting node.
RVAR_UTK_SGRP_ID	Char	8	413	420	The submitting group name.
RVAR_UTK_SPOE	Char	8	422	429	The port of entry.
RVAR_UTK_SPCLASS	Char	8	431	438	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
RVAR_UTK_USER_ID	Char	8	440	447	User ID associated with the record.
RVAR_UTK_GRP_ID	Char	8	449	456	Group name associated with the record.
RVAR_UTK_DFT_GRP	Yes/No	4	458	461	Is a default group assigned?
RVAR_UTK_DFT_SECL	Yes/No	4	463	466	Is a default SECLABEL assigned?
RVAR_APPC_LINK	Char	16	468	483	Key to link together APPC records.
RVAR_SPECIFIED	Char	1024	485	1508	The keywords specified.
RVAR_FAILED	Char	1024	1510	2533	The keywords that failed.
RVAR_UTK_NETW	Char	8	2535	2542	The port of entry network name.
RVAR_X500_SUBJECT	Char	255	2544	2798	Subject's name associated with this event.
RVAR_X500_ISSUER	Char	255	2800	3054	Issuer's name associated with this event.

Event Qualifiers for RVAR Y Commands

The event qualifiers that may be associated with a RVAR Y command are shown in Table 53.

Table 53. Event Qualifiers for RVAR Y Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	No violations detected.
INSAUTH	01	Insufficient authority.
KEYWVIOL	02	Keyword violation.

The Format of the APPCLU Record Extension

Table 54 describes the format of a record that is created by the auditing of an APPCLU resource.

Table 54. Format of the APPCLU Record Extension (Event Code 26)

Field Name	Type	Length	Position		Comments
			Start	End	
APPC_RES_NAME	Char	255	282	536	Resource name.
APPC_CLASS	Char	8	538	545	Class name.
APPC_TYPE	Char	8	547	554	Type of resource data. Valid values are "RESOURCE" if ACC_NAME is a generic resource name, and "PROFILE" if ACC_NAME is a generic profile.
APPC_NAME	Char	246	556	801	Resource or profile name.
APPC_OWN_ID	Char	8	803	810	Name of the profile owner.
APPC_USER_NAME	Char	20	812	831	User name.
APPC_UTK_ENCR	Yes/No	4	833	836	Is the UTOKEN associated with this user encrypted?
APPC_UTK_PRE19	Yes/No	4	838	841	Is this a pre-1.9 token?
APPC_UTK_VERPROF	Yes/No	4	843	846	Is the VERIFYX propagation flag set?
APPC_UTK_NJEUNUSR	Yes/No	4	848	851	Is this the NJE undefined user?
APPC_UTK_LOGUSR	Yes/No	4	853	856	Is UAUDIT specified for this user?
APPC_UTK_SPECIAL	Yes/No	4	858	861	Is this a SPECIAL user?
APPC_UTK_DEFAULT	Yes/No	4	863	866	Is this a default token?
APPC_UTK_UNKNUSR	Yes/No	4	868	871	Is this an undefined user?
APPC_UTK_ERROR	Yes/No	4	873	876	Is this user token in error?
APPC_UTK_TRUSTED	Yes/No	4	878	881	Is this user a part of the trusted computing base (TCB)?
APPC_UTK_SESTYPE	Char	8	883	890	The session type of this session.
APPC_UTK_SURROGAT	Yes/No	4	892	895	Is this a surrogate user?
APPC_UTK_REMOTE	Yes/No	4	897	900	Is this a remote job?
APPC_UTK_PRIV	Yes/No	4	902	905	Is this a privileged user ID?
APPC_UTK_SECL	Char	8	907	914	The SECLABEL of the user.
APPC_UTK_EXECNODE	Char	8	916	923	The execution node of the work.
APPC_UTK_SUSER_ID	Char	8	925	932	The submitting user ID.
APPC_UTK_SNODE	Char	8	934	941	The submitting node.
APPC_UTK_SGRP_ID	Char	8	943	950	The submitting group name.
APPC_UTK_SPOE	Char	8	952	959	The port of entry.

Table 54. Format of the APPCLU Record Extension (Event Code 26) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
APPC_UTK_SPCLASS	Char	8	961	968	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
APPC_UTK_USER_ID	Char	8	970	977	User ID associated with the record.
APPC_UTK_GRP_ID	Char	8	979	986	Group name associated with the record.
APPC_UTK_DFT_GRP	Yes/No	4	988	991	Is a default group assigned?
APPC_UTK_DFT_SECL	Yes/No	4	993	996	Is a default SECLABEL assigned?
APPC_APPC_LINK	Char	16	998	1013	Key to link together APPC records.
APPC_UTK_NETW	Char	8	1015	1022	The port of entry network name.
APPC_X500_SUBJECT	Char	255	1024	1278	Subject's name associated with this event.
APPC_X500_ISSUER	Char	255	1280	1534	Issuer's name associated with this event.

Event Qualifiers for APPCLU (APPC Session Establishment) Records

The event qualifiers that may be associated with a APPCLU event are shown in Table 55.

Table 55. Event Qualifiers for APPC Session Establishment Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Partner verification OK.
NOVERIFY	01	Session established without verification.
LKEYEXPR	02	Local key expires in less than 5 days.
REVOKED	03	Partner LU access has been revoked.
NOMATCH	04	Partner LU key does not match this LU key.
TRMSECUR	05	Session terminated for security reasons.
NOSESKEY	06	Required session key not defined.
LUATTACK	07	Possible security attack by partner LU.
NOPRTKEY	08	Session key not defined for the partner LU.
NOKEY	09	Session key not defined for this LU.
SNAERROR	10	SNA security-related session
PROFCHNG	11	Profile changed during verification.
SKEYEXPR	12	Expired session key error.

The Format of the General Event Record Extension

Table 56 describes the format of a record that is created by a general event.

Table 56. Format of the General Event Record Extension (Event Code 27)

Field Name	Type	Length	Position		Comments
			Start	End	
GEN_CLASS	Char	8	282	289	Class name.
GEN_LOGSTR	Char	255	291	545	LOGSTR= data from the RACROUTE
GEN_USER_NAME	Char	20	547	566	User name.
GEN_UTK_ENCR	Yes/No	4	568	571	Is the UTOKEN associated with this user encrypted?
GEN_UTK_PRE19	Yes/No	4	573	576	Is this a pre-1.9 token?

SMF Data Unload—IRRADU00

Table 56. Format of the General Event Record Extension (Event Code 27) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
GEN_UTK_VERPROF	Yes/No	4	578	581	Is the VERIFYX propagation flag set?
GEN_UTK_NJEUNUSR	Yes/No	4	583	586	Is this the NJE undefined user?
GEN_UTK_LOGUSR	Yes/No	4	588	591	Is UAUDIT specified for this user?
GEN_UTK_SPECIAL	Yes/No	4	593	596	Is this a SPECIAL user?
GEN_UTK_DEFAULT	Yes/No	4	598	601	Is this a default token?
GEN_UTK_UNKNUSR	Yes/No	4	603	606	Is this an undefined user?
GEN_UTK_ERROR	Yes/No	4	608	611	Is this user token in error?
GEN_UTK_TRUSTED	Yes/No	4	613	616	Is this user a part of the trusted computing base (TCB)?
GEN_UTK_SESSTYPE	Char	8	618	625	The session type of this session.
GEN_UTK_SURROGAT	Yes/No	4	627	630	Is this a surrogate user?
GEN_UTK_REMOTE	Yes/No	4	632	635	Is this a remote job?
GEN_UTK_PRIV	Yes/No	4	637	640	Is this a privileged user ID?
GEN_UTK_SECL	Char	8	642	649	The SECLABEL of the user.
GEN_UTK_EXECNODE	Char	8	651	658	The execution node of the work.
GEN_UTK_SUSER_ID	Char	8	660	667	The submitting user ID.
GEN_UTK_SNODE	Char	8	669	676	The submitting node.
GEN_UTK_SGRP_ID	Char	8	678	685	The submitting group name.
GEN_UTK_SPOE	Char	8	687	694	The port of entry.
GEN_UTK_SPCLASS	Char	8	696	703	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
GEN_UTK_USER_ID	Char	8	705	712	User ID associated with the record.
GEN_UTK_GRP_ID	Char	8	714	721	Group name associated with the record.
GEN_UTK_DFT_GRP	Yes/No	4	723	726	Is a default group assigned?
GEN_UTK_DFT_SECL	Yes/No	4	728	731	Is a default SECLABEL assigned?
GEN_APPC_LINK	Char	16	733	748	Key to link together GENERAL records.
GEN_UTK_NETW	Char	8	750	757	The port of entry network name.
GEN_X500_SUBJECT	Char	255	759	1013	Subject's name associated with this event.
GEN_X500_ISSUER	Char	255	1015	1269	Issuer's name associated with this event.

Event Qualifiers for General Events

The event qualifiers that may be associated with a general event are determined by the installation. These event codes will be unloaded as integer values.

The Format of the Directory Search Record Extension

Table 57 describes the format of a record that is created by a directory search event.

Table 57. Format of the Directory Search Record Extension (Event Code 28)

Field Name	Type	Length	Position		Comments
			Start	End	
DSCH_CLASS	Char	8	282	289	Class name.
DSCH_USER_NAME	Char	20	291	310	The name associated with the user ID.
DSCH_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?

Table 57. Format of the Directory Search Record Extension (Event Code 28) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
DSCH_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
DSCH_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
DSCH_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
DSCH_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
DSCH_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
DSCH_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
DSCH_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
DSCH_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
DSCH_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
DSCH_UTK_SESTYPE	Char	8	362	369	The session type of this session.
DSCH_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
DSCH_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
DSCH_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
DSCH_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
DSCH_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
DSCH_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
DSCH_UTK_SNODE	Char	8	413	420	The submitting node.
DSCH_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
DSCH_UTK_SPOE	Char	8	431	438	The port of entry.
DSCH_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
DSCH_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
DSCH_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
DSCH_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
DSCH_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
DSCH_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
DSCH_AUDIT_CODE	Char	11	494	504	Audit function code.
DSCH_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
DSCH_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
DSCH_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
DSCH_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
DSCH_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
DSCH_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
DSCH_PATH_NAME	Char	1023	572	1594	The requested path name.
DSCH_FILE_ID	Char	32	1596	1627	File ID.
DSCH_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
DSCH_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
DSCH_REQUEST_READ	Yes/No	4	1651	1654	Did the requested access include read?
DSCH_REQUEST_WRITE	Yes/No	4	1656	1659	Did the requested access include write?
DSCH_REQUEST_EXEC	Yes/No	4	1661	1664	Did the requested access include EXECUTE?
DSCH_REQUEST_DSRCH	Yes/No	4	1666	1669	Did the requested access include directory search?

SMF Data Unload—IRRADU00

Table 57. Format of the Directory Search Record Extension (Event Code 28) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
DSCH_ACCESS_TYPE	Char	8	1671	1678	What bits were used in granting the access? Valid values are "OWNER", "GROUP", "OTHER", "ACLUSER", "ACLGROUP", "ACLERROR", and "RSTD".
DSCH_ALLOWED_READ	Yes/No	4	1680	1683	Was read access allowed?
DSCH_ALLOWED_WRITE	Yes/No	4	1685	1688	Was write access allowed?
DSCH_ALLOWED_EXEC	Yes/No	4	1690	1693	Was execute or search access allowed?
DSCH_REQUEST_PATH2	Char	1023	1695	2717	Second requested path name.
DSCH_SERVICE_CODE	Char	11	2719	2729	The service that was being processed. This is set only when the DSCH_AUDIT_CODE is "LOOKUP".
DSCH_HFS_DS_NAME	Char	44	2731	2774	HFS data set name for the mounted file system.
DSCH_SYMLINK	Char	1023	2776	3798	The content of SYMLINK.
DSCH_FILE_NAME	Char	256	3800	4055	The file name that is being checked.
DSCH_PATH_TYPE	Char	4	4057	4060	Type of the requested path name. Valid values are "OLD" and "NEW".
DSCH_FILEPOOL	Char	8	4062	4069	SFS filepool containing the BFS file.
DSCH_FILESPACE	Char	8	4071	4078	SFS filespace containing the BFS file.
DSCH_INODE	Integer	10	4080	4089	Inode (file serial number).
DSCH_SCID	Integer	10	4091	4100	File SCID.
DSCH_DCE_LINK	Char	16	4102	4117	Link to connect DCE records that originate from a single DCE request.
DSCH_AUTH_TYPE	Char	13	4119	4131	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
DSCH_DFLT_PROCESS	Yes/No	4	4133	4136	Default z/OS UNIX security environment in effect.
DSCH_UTK_NETW	CHAR	8	4138	4145	The port of entry network name.
DSCH_X500_SUBJECT	Char	255	4147	4401	Subject's name associated with this event.
DSCH_X500_ISSUER	Char	255	4403	4657	Issuer's name associated with this event.

Event Qualifiers for Directory Search Records

The event qualifiers that may be associated with a directory search event are shown in Table 58.

Table 58. Event Qualifiers for Directory Search Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Access allowed.
NOTAUTH	01	Not authorized to search the directory.

The Format of the Check Directory Access Record Extension

Table 59 describes the format of a record that is created by checking access to a directory.

Table 59. Format of the Check Directory Access Record Extension (Event Code 29)

Field Name	Type	Length	Position		Comments
			Start	End	
DACC_CLASS	Char	8	282	289	Class name.

Table 59. Format of the Check Directory Access Record Extension (Event Code 29) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
DACC_USER_NAME	Char	20	291	310	The name associated with the user ID.
DACC_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
DACC_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
DACC_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
DACC_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
DACC_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
DACC_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
DACC_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
DACC_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
DACC_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
DACC_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
DACC_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
DACC_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
DACC_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
DACC_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
DACC_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
DACC_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
DACC_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
DACC_UTK_SNODE	Char	8	413	420	The submitting node.
DACC_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
DACC_UTK_SPOE	Char	8	431	438	The port of entry.
DACC_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
DACC_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
DACC_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
DACC_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
DACC_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
DACC_APPC_LINK	Char	16	477	492	Key to link together APPC records.
DACC_AUDIT_CODE	Char	11	494	504	Audit function code.
DACC_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
DACC_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
DACC_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
DACC_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
DACC_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
DACC_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
DACC_PATH_NAME	Char	1023	572	1594	The requested path name.
DACC_FILE_ID	Char	32	1596	1627	File ID.
DACC_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
DACC_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
DACC_REQUEST_READ	Yes/No	4	1651	1654	Did the requested access include read?
DACC_REQUEST_WRITE	Yes/No	4	1656	1659	Did the requested access include write?

SMF Data Unload—IRRADU00

Table 59. Format of the Check Directory Access Record Extension (Event Code 29) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
DACC_REQUEST_EXEC	Yes/No	4	1661	1664	Did the requested access include execute?
DACC_REQUEST_DSRCH	Yes/No	4	1666	1669	Did the requested access include directory search?
DACC_ACCESS_TYPE	Char	8	1671	1678	What bits were used in granting the access? Valid values are "OWNER", "GROUP", "OTHER", "ACLUSER", "ACLGROUP", "ACLERROR", and "RSTD".
DACC_ALLOWED_READ	Yes/No	4	1680	1683	Was read access allowed?
DACC_ALLOWED_WRITE	Yes/No	4	1685	1688	Was write access allowed?
DACC_ALLOWED_EXEC	Yes/No	4	1690	1693	Was execute access allowed?
DACC_REQUEST_PATH2	Char	1023	1695	2717	Second requested path name.
DACC_SYMLINK	Char	1023	2719	3741	The content of SYMLINK.
DACC_FILE_NAME	Char	256	3743	3998	The file name that is being checked.
DACC_PATH_TYPE	Char	4	4000	4003	Type of the requested path name. Valid values are "OLD" and "NEW".
DACC_FILEPOOL	Char	8	4005	4012	SFS filepool containing the BFS file.
DACC_FILESPACE	Char	8	4014	4021	SFS filespace containing the BFS file.
DACC_INODE	Integer	10	4023	4032	Inode (file serial number).
DACC_SCID	Integer	10	4034	4043	File SCID.
DACC_DCE_LINK	Char	16	4045	4060	Link to connect DCE records that originate from a single DCE request.
DACC_AUTH_TYPE	Char	13	4062	4074	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
DACC_DFLT_PROCESS	Yes/No	4	4076	4079	Default z/OS UNIX security environment in effect.
DACC_UTK_NETW	Char	8	4081	4088	The port of entry network name.
DACC_X500_SUBJECT	Char	255	4090	4344	Subject's name associated with this event.
DACC_X500_ISSUER	Char	255	4346	4600	Issuer's name associated with this event.

Event Qualifiers for Check Directory Access Records

The event qualifiers that may be associated with a directory search event are shown in Table 60.

Table 60. Event Qualifiers for Check Directory Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Access allowed.
NOTAUTH	01	Not authorized to the directory.

The Format of the Check File Access Record Extension

Table 61 describes the format of a record that is created by checking access to a file.

Table 61. Format of the Check File Access Record Extension (Event Code 30)

Field Name	Type	Length	Position		Comments
			Start	End	
FACC_CLASS	Char	8	282	289	Class name.

Table 61. Format of the Check File Access Record Extension (Event Code 30) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
FACC_USER_NAME	Char	20	291	310	The name associated with the user ID.
FACC_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
FACC_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
FACC_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
FACC_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
FACC_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
FACC_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
FACC_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
FACC_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
FACC_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
FACC_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
FACC_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
FACC_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
FACC_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
FACC_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
FACC_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
FACC_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
FACC_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
FACC_UTK_SNODE	Char	8	413	420	The submitting node.
FACC_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
FACC_UTK_SPOE	Char	8	431	438	The port of entry.
FACC_UTK_SPCCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
FACC_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
FACC_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
FACC_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
FACC_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
FACC_APPC_LINK	Char	16	477	492	Key to link together APPC records.
FACC_AUDIT_CODE	Char	11	494	504	Audit function code.
FACC_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
FACC_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
FACC_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
FACC_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
FACC_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
FACC_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
FACC_PATH_NAME	Char	1023	572	1594	The requested path name.
FACC_FILE_ID	Char	32	1596	1627	File ID.
FACC_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
FACC_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
FACC_REQUEST_READ	Yes/No	4	1651	1654	Did the requested access include read?
FACC_REQUEST_WRITE	Yes/No	4	1656	1659	Did the requested access include write?

SMF Data Unload—IRRADU00

Table 61. Format of the Check File Access Record Extension (Event Code 30) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
FACC_REQUEST_EXEC	Yes/No	4	1661	1664	Did the requested access include EXECUTE?
FACC_REQUEST_DSRCH	Yes/No	4	1666	1669	Did the requested access include directory search?
FACC_ACCESS_TYPE	Char	8	1671	1678	What bits were used in granting the access? Valid values are "OWNER", "GROUP", "OTHER", "ACLUSER", "ACLGROUP", "ACLERROR", and "RSTD".
FACC_ALLOWED_READ	Yes/No	4	1680	1683	Was read access allowed?
FACC_ALLOWED_WRITE	Yes/No	4	1685	1688	Was write access allowed?
FACC_ALLOWED_EXEC	Yes/No	4	1690	1693	Was execute access allowed?
FACC_REQUEST_PATH2	Char	1023	1695	2717	Second requested path name.
FACC_FILE_NAME	Char	256	2719	2974	The file name that is being checked.
FACC_PATH_TYPE	Char	4	2976	2979	Type of the requested path name. Valid values are "OLD" and "NEW".
FACC_FILEPOOL	Char	8	2981	2988	SFS filepool containing the BFS file.
FACC_FILESPACE	Char	8	2990	2997	SFS filespace containing the BFS file.
FACC_INODE	Integer	10	2999	3008	Inode (file serial number).
FACC_SCID	Integer	10	3010	3019	File SCID.
FACC_DCE_LINK	Char	16	3021	3036	Link to connect DCE records that originate from a single DCE request.
FACC_AUTH_TYPE	Char	13	3038	3050	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
FACC_DFLT_PROCESS	Yes/No	4	3052	3055	Default z/OS UNIX security environment in effect.
FACC_UTK_NETW	Char	8	3057	3064	The port of entry network name.
FACC_X500_SUBJECT	Char	255	3066	3320	Subject's name associated with this event.
FACC_X500_ISSUER	Char	255	3322	3576	Issuer's name associated with this event.

Event Qualifiers for Check File Access Records

The event qualifiers that may be associated with a check file access event are shown in Table 62.

Table 62. Event Qualifiers for Check File Access Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Access allowed.
NOTAUTH	01	Not authorized to the file.

The Format of the Change Audit Record Extension

Table 63 describes the format of a record that is created by checking access to a file.

Table 63. Format of the Change Audit Record Extension (Event Code 31)

Field Name	Type	Length	Position		Comments
			Start	End	
CAUD_CLASS	Char	8	282	289	Class name.
CAUD_USER_NAME	Char	20	291	310	The name associated with the user ID.

Table 63. Format of the Change Audit Record Extension (Event Code 31) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
CAUD_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
CAUD_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
CAUD_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
CAUD_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
CAUD_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
CAUD_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
CAUD_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
CAUD_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
CAUD_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
CAUD_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
CAUD_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
CAUD_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
CAUD_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
CAUD_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
CAUD_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
CAUD_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
CAUD_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
CAUD_UTK_SNODE	Char	8	413	420	The submitting node.
CAUD_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
CAUD_UTK_SPOE	Char	8	431	438	The port of entry.
CAUD_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
CAUD_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
CAUD_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
CAUD_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
CAUD_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
CAUD_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
CAUD_AUDIT_CODE	Char	11	494	504	Audit function code.
CAUD_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
CAUD_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
CAUD_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
CAUD_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
CAUD_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
CAUD_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
CAUD_PATH_NAME	Char	1023	572	1594	The requested path name.
CAUD_FILE_ID	Char	32	1596	1627	File ID.
CAUD_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
CAUD_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
CAUD_REQUEST_READ	Char	8	1651	1658	What audit options are requested for a READ operation? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".

SMF Data Unload—IRRADU00

Table 63. Format of the Change Audit Record Extension (Event Code 31) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
CAUD_REQUEST_WRITE	Char	8	1660	1667	What audit options are requested for a WRITE operation? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
CAUD_REQUEST_EXEC	Char	8	1669	1676	What audit options are requested for an EXECUTE operation? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
CAUD_UOLD_READ	Char	8	1678	1685	What were the previous user audit options for READ actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
CAUD_UOLD_WRITE	Char	8	1687	1694	What were the previous user audit options for WRITE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
CAUD_UOLD_EXEC	Char	8	1696	1703	What were the previous user audit options for EXECUTE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
CAUD_AOLD_READ	Char	8	1705	1712	What were the previous auditor audit options for READ actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
CAUD_AOLD_WRITE	Char	8	1714	1721	What were the previous auditor audit options for WRITE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
CAUD_AOLD_EXEC	Char	8	1723	1730	What were the previous auditor audit options for EXECUTE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
CAUD_UNEW_READ	Char	8	1732	1739	What are the new user audit options for READ actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
CAUD_UNEW_WRITE	Char	8	1741	1748	What are the new user audit options for WRITE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
CAUD_UNEW_EXEC	Char	8	1750	1757	What are the new user audit options for EXECUTE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
CAUD_ANEW_READ	Char	8	1759	1766	What are the new auditor audit options for READ actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
CAUD_ANEW_WRITE	Char	8	1768	1775	What are the new auditor audit options for WRITE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
CAUD_ANEW_EXEC	Char	8	1777	1784	What are the new auditor audit options for EXECUTE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
CAUD_FILEPOOL	Char	8	1786	1793	SFS filepool containing the BFS file.
CAUD_FILESPACE	Char	8	1795	1802	SFS filespace containing the BFS file.
CAUD_INODE	Integer	10	1804	1813	Inode (file serial number).
CAUD_SCID	Integer	10	1815	1824	File SCID.
CAUD_DCE_LINK	Char	16	1826	1841	Link to connect DCE records that originate from a single DCE request.
CAUD_AUTH_TYPE	Char	13	1843	1855	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
CAUD_DFLT_PROCESS	Yes/No	4	1857	1860	Default z/OS UNIX security environment in effect.
CAUD_UTK_NETW	Char	8	1862	1869	The port of entry network name.
CAUD_X500_SUBJECT	Char	255	1871	2125	Subject's name associated with this event.

Table 63. Format of the Change Audit Record Extension (Event Code 31) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
CAUD_X500_ISSUER	Char	255	2127	2381	Issuer's name associated with this event.

Event Qualifiers for Change Audit Records

The event qualifiers that may be associated with a directory search event are shown in Table 64.

Table 64. Event Qualifiers for Change Audit Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	File's audit options changed.
NOTAUTHU	01	Not authorized to change the user audit options on the specified file.
NOTAUTHA	02	Not authorized to change the auditor audit options on the specified file.

The Format of the Change Directory Record Extension

Table 65 describes the format of a record that is created by changing directories.

Table 65. Format of the Change Directory Record Extension (Event Code 32)

Field Name	Type	Length	Position		Comments
			Start	End	
CDIR_CLASS	Char	8	282	289	Class name.
CDIR_USER_NAME	Char	20	291	310	The name associated with the user ID.
CDIR_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
CDIR_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
CDIR_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
CDIR_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
CDIR_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
CDIR_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
CDIR_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
CDIR_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
CDIR_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
CDIR_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
CDIR_UTK_SESTYPE	Char	8	362	369	The session type of this session.
CDIR_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
CDIR_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
CDIR_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
CDIR_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
CDIR_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
CDIR_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
CDIR_UTK_SNODE	Char	8	413	420	The submitting node.
CDIR_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
CDIR_UTK_SPOE	Char	8	431	438	The port of entry.

SMF Data Unload—IRRADU00

Table 65. Format of the Change Directory Record Extension (Event Code 32) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
CDIR_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
CDIR_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
CDIR_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
CDIR_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
CDIR_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
CDIR_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
CDIR_AUDIT_CODE	Char	11	494	504	Audit function code.
CDIR_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
CDIR_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
CDIR_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
CDIR_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
CDIR_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
CDIR_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
CDIR_PATH_NAME	Char	1023	572	1594	The requested path name.
CDIR_FILE_ID	Char	32	1596	1627	File ID.
CDIR_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
CDIR_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
CDIR_DCE_LINK	Char	16	1651	1666	Link to connect DCE records that originate from a single DCE request.
CDIR_AUTH_TYPE	Char	13	1668	1680	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
CDIR_DFLT_PROCESS	Yes/No	4	1682	1685	Default z/OS UNIX security environment in effect.
CDIR_UTK_NETW	Char	8	1687	1694	The port of entry network name.
CDIR_X500_SUBJECT	Char	255	1696	1950	Subject's name associated with this event.
CDIR_X500_ISSUER	Char	255	1952	2206	Issuer's name associated with this event.

Event Qualifiers for Change Directory Records

The event qualifiers that may be associated with a directory search event are shown in Table 66.

Table 66. Event Qualifiers for Change Directory Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Current working directory changed. Failures are logged as directory search events.

The Format of the Change File Mode Record Extension

Table 67 on page 167 describes the format of a record that is created by changing the access mode of a file.

Table 67. Format of the Change File Mode Record Extension (Event Code 33)

Field Name	Type	Length	Position		Comments
			Start	End	
CMOD_CLASS	Char	8	282	289	Class name.
CMOD_USER_NAME	Char	20	291	310	The name associated with the user ID.
CMOD_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
CMOD_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
CMOD_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
CMOD_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
CMOD_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
CMOD_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
CMOD_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
CMOD_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
CMOD_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
CMOD_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
CMOD_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
CMOD_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
CMOD_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
CMOD_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
CMOD_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
CMOD_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
CMOD_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
CMOD_UTK_SNODE	Char	8	413	420	The submitting node.
CMOD_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
CMOD_UTK_SPOE	Char	8	431	438	The port of entry.
CMOD_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
CMOD_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
CMOD_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
CMOD_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
CMOD_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
CMOD_APPC_LINK	Char	16	477	492	Key to link together APPC records.
CMOD_AUDIT_CODE	Char	11	494	504	Audit function code.
CMOD_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
CMOD_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
CMOD_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
CMOD_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
CMOD_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
CMOD_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
CMOD_PATH_NAME	Char	1023	572	1594	The requested path name.
CMOD_FILE_ID	Char	32	1596	1627	File ID.
CMOD_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
CMOD_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
CMOD_OLD_S_ISGID	Yes/No	4	1651	1654	Was the S_ISGID bit requested on for this file?

SMF Data Unload—IRRADU00

Table 67. Format of the Change File Mode Record Extension (Event Code 33) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
CMOD_OLD_S_ISUID	Yes/No	4	1656	1659	Was the S_ISUID bit requested on for this file?
CMOD_OLD_S_ISVTX	Yes/No	4	1661	1664	Was the S_ISVTX bit requested on for this file?
CMOD_OLD_OWN_READ	Yes/No	4	1666	1669	Was the owner READ bit on for this file?
CMOD_OLD_OWN_WRITE	Yes/No	4	1671	1674	Was the owner WRITE bit on for this file?
CMOD_OLD_OWN_EXEC	Yes/No	4	1676	1679	Was the owner EXECUTE bit on for this file?
CMOD_OLD_GRP_READ	Yes/No	4	1681	1684	Was the group READ bit on for this file?
CMOD_OLD_GRP_WRITE	Yes/No	4	1686	1689	Was the group WRITE bit on for this file?
CMOD_OLD_GRP_EXEC	Yes/No	4	1691	1694	Was the group EXECUTE bit on for this file?
CMOD_OLD_OTH_READ	Yes/No	4	1696	1699	Was the other READ bit on for this file?
CMOD_OLD_OTH_WRITE	Yes/No	4	1701	1704	Was the other WRITE bit on for this file?
CMOD_OLD_OTH_EXEC	Yes/No	4	1706	1709	Was the other EXECUTE bit on for this file?
CMOD_NEW_S_ISGID	Yes/No	4	1711	1714	Is the S_ISGID bit requested on for this file?
CMOD_NEW_S_ISUID	Yes/No	4	1716	1719	Is the S_ISUID bit requested on for this file?
CMOD_NEW_S_ISVTX	Yes/No	4	1721	1724	Is the S_ISVTX bit requested on for this file?
CMOD_NEW_OWN_READ	Yes/No	4	1726	1729	Is the owner READ bit on for this file?
CMOD_NEW_OWN_WRITE	Yes/No	4	1731	1734	Is the owner WRITE bit on for this file?
CMOD_NEW_OWN_EXEC	Yes/No	4	1736	1739	Is the owner EXECUTE bit on for this file?
CMOD_NEW_GRP_READ	Yes/No	4	1741	1744	Is the group READ bit on for this file?
CMOD_NEW_GRP_WRITE	Yes/No	4	1746	1749	Is the group WRITE bit on for this file?
CMOD_NEW_GRP_EXEC	Yes/No	4	1751	1754	Is the group EXECUTE bit on for this file?
CMOD_NEW_OTH_READ	Yes/No	4	1756	1759	Is the other READ bit on for this file?
CMOD_NEW_OTH_WRITE	Yes/No	4	1761	1764	Is the other WRITE bit on for this file?
CMOD_NEW_OTH_EXEC	Yes/No	4	1766	1769	Is the other EXECUTE bit on for this file?
CMOD_REQ_S_ISGID	Yes/No	4	1771	1774	Was the S_ISGID bit requested on for this file?
CMOD_REQ_S_ISUID	Yes/No	4	1776	1779	Was the S_ISUID bit requested on for this file?
CMOD_REQ_S_ISVTX	Yes/No	4	1781	1784	Was the S_ISVTX bit requested on for this file?
CMOD_REQ_OWN_READ	Yes/No	4	1786	1789	Was the owner READ bit requested on for this file?
CMOD_REQ_OWN_WRITE	Yes/No	4	1791	1794	Was the owner WRITE bit requested on for this file?
CMOD_REQ_OWN_EXEC	Yes/No	4	1796	1799	Was the owner EXECUTE bit requested on for this file?
CMOD_REQ_GRP_READ	Yes/No	4	1801	1804	Was the group READ bit requested on for this file?
CMOD_REQ_GRP_WRITE	Yes/No	4	1806	1809	Was the group WRITE bit requested on for this file?
CMOD_REQ_GRP_EXEC	Yes/No	4	1811	1814	Was the group EXECUTE bit requested on for this file?
CMOD_REQ_OTH_READ	Yes/No	4	1816	1819	Was the other READ bit requested on for this file?
CMOD_REQ_OTH_WRITE	Yes/No	4	1821	1824	Was the other WRITE bit requested on for this file?
CMOD_REQ_OTH_EXEC	Yes/No	4	1826	1829	Was the other EXECUTE bit requested on for this file?
CMOD_FILEPOOL	Char	8	1831	1838	SFS filepool containing the BFS file.
CMOD_FILESPACE	Char	8	1840	1847	SFS filespace containing the BFS file.
CMOD_INODE	Integer	10	1849	1858	Inode (file serial number).

Table 67. Format of the Change File Mode Record Extension (Event Code 33) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
CMOD_SCID	Integer	10	1860	1869	File SCID.
CMOD_DCE_LINK	Char	16	1871	1886	Link to connect DCE records that originate from a single DCE request.
CMOD_AUTH_TYPE	Char	13	1888	1900	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
CMOD_DFLT_PROCESS	Yes/No	4	1902	1905	Default z/OS UNIX security environment in effect.
CMOD_UTK_NETW	Char	8	1907	1914	The port of entry network name.
CMOD_X500_SUBJECT	Char	255	1916	2170	Subject's name associated with this event.
CMOD_X500_ISSUER	Char	255	2172	2426	Issuer's name associated with this event.

Event Qualifiers for Change File Mode Records

The event qualifiers that may be associated with changing a file mode event are shown in Table 68.

Table 68. Event Qualifiers for Change File Mode Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	File's mode changed.
NOTAUTH	01	Not authorized to change the file's mode.

The Format of the Change File Ownership Record Extension

Table 69 describes the format of a record that is created by changing the ownership of a file.

Table 69. Format of the Change File Ownership Record Extension (Event Code 34)

Field Name	Type	Length	Position		Comments
			Start	End	
COWN_CLASS	Char	8	282	289	Class name.
COWN_USER_NAME	Char	20	291	310	The name associated with the user ID.
COWN_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
COWN_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
COWN_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
COWN_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
COWN_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
COWN_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
COWN_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
COWN_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
COWN_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
COWN_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
COWN_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
COWN_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
COWN_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
COWN_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?

SMF Data Unload—IRRADU00

Table 69. Format of the Change File Ownership Record Extension (Event Code 34) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
COWN_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
COWN_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
COWN_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
COWN_UTK_SNODE	Char	8	413	420	The submitting node.
COWN_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
COWN_UTK_SPOE	Char	8	431	438	The port of entry.
COWN_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
COWN_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
COWN_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
COWN_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
COWN_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
COWN_APPC_LINK	Char	16	477	492	Key to link together APPC records.
COWN_AUDIT_CODE	Char	11	494	504	Audit function code.
COWN_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
COWN_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
COWN_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
COWN_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
COWN_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
COWN_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
COWN_PATH_NAME	Char	1023	572	1594	The requested path name.
COWN_FILE_ID	Char	32	1596	1627	File ID.
COWN_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
COWN_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
COWN_UID	Integer	10	1651	1660	The z/OS UNIX user identifier (UID) input parameter.
COWN_GID	Integer	10	1662	1671	The z/OS UNIX group identifier (GID) input parameter.
COWN_FILEPOOL	Char	8	1673	1680	SFS filepool containing the BFS file.
COWN_FILESPACE	Char	8	1682	1689	SFS filespace containing the BFS file.
COWN_INODE	Integer	10	1691	1700	Inode (file serial number).
COWN_SCID	Integer	10	1702	1711	File SCID.
COWN_DCE_LINK	Char	16	1713	1728	Link to connect DCE records that originate from a single DCE request.
COWN_AUTH_TYPE	Char	13	1730	1742	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
COWN_DFLT_PROCESS	Yes/No	4	1744	1747	Default z/OS UNIX security environment in effect.
COWN_UTK_NETW	Char	8	1749	1756	The port of entry network name.
COWN_X500_SUBJECT	Char	255	1758	2012	Subject's name associated with this event.
COWN_X500_ISSUER	Char	255	2014	2268	Issuer's name associated with this event.

Event Qualifiers for Change File Ownership Records

The event qualifiers that may be associated with changing a file's ownership are shown in Table 70.

Table 70. Event Qualifiers for Change File Ownership Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	File's ownership changed.
NOTAUTH	01	Not authorized to change the file's ownership.

The Format of the Clear SETID Bits Record Extension

Table 71 describes the format of a record that is created by clearing the SETID bits of a file.

Table 71. Format of the Clear SETID Bits Record Extension (Event Code 35)

Field Name	Type	Length	Position		Comments
			Start	End	
CSID_CLASS	Char	8	282	289	Class name.
CSID_USER_NAME	Char	20	291	310	The name associated with the user ID.
CSID_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
CSID_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
CSID_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
CSID_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
CSID_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
CSID_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
CSID_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
CSID_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
CSID_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
CSID_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
CSID_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
CSID_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
CSID_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
CSID_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
CSID_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
CSID_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
CSID_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
CSID_UTK_SNODE	Char	8	413	420	The submitting node.
CSID_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
CSID_UTK_SPOE	Char	8	431	438	The port of entry.
CSID_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
CSID_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
CSID_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
CSID_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
CSID_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
CSID_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.

SMF Data Unload—IRRADU00

Table 71. Format of the Clear SETID Bits Record Extension (Event Code 35) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
CSID_AUDIT_CODE	Char	11	494	504	Audit function code.
CSID_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
CSID_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
CSID_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
CSID_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
CSID_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
CSID_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
CSID_PATH_NAME	Char	1023	572	1594	The requested path name.
CSID_FILE_ID	Char	32	1596	1627	File ID.
CSID_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
CSID_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
CSID_OLD_S_ISGID	Yes/No	4	1651	1654	Was the S_ISGID bit requested on for this file?
CSID_OLD_S_ISUID	Yes/No	4	1656	1659	Was the S_ISUID bit requested on for this file?
CSID_OLD_S_ISVTX	Yes/No	4	1661	1664	Was the S_ISVTX bit requested on for this file?
CSID_OLD_OWN_READ	Yes/No	4	1666	1669	Was the owner READ bit on for this file?
CSID_OLD_OWN_WRITE	Yes/No	4	1671	1674	Was the owner WRITE bit on for this file?
CSID_OLD_OWN_EXEC	Yes/No	4	1676	1679	Was the owner EXECUTE bit on for this file?
CSID_OLD_GRP_READ	Yes/No	4	1681	1684	Was the group READ bit on for this file?
CSID_OLD_GRP_WRITE	Yes/No	4	1686	1689	Was the group WRITE bit on for this file?
CSID_OLD_GRP_EXEC	Yes/No	4	1691	1694	Was the group EXECUTE bit on for this file?
CSID_OLD_OTH_READ	Yes/No	4	1696	1699	Was the other READ bit on for this file?
CSID_OLD_OTH_WRITE	Yes/No	4	1701	1704	Was the other WRITE bit on for this file?
CSID_OLD_OTH_EXEC	Yes/No	4	1706	1709	Was the other EXECUTE bit on for this file?
CSID_NEW_S_ISGID	Yes/No	4	1711	1714	Is the S_ISGID bit requested on for this file?
CSID_NEW_S_ISUID	Yes/No	4	1716	1719	Is the S_ISUID bit requested on for this file?
CSID_NEW_S_ISVTX	Yes/No	4	1721	1724	Is the S_ISVTX bit requested on for this file?
CSID_NEW_OWN_READ	Yes/No	4	1726	1729	Is the owner READ bit on for this file?
CSID_NEW_OWN_WRITE	Yes/No	4	1731	1734	Is the owner WRITE bit on for this file?
CSID_NEW_OWN_EXEC	Yes/No	4	1736	1739	Is the owner EXECUTE bit on for this file?
CSID_NEW_GRP_READ	Yes/No	4	1741	1744	Is the group READ bit on for this file?
CSID_NEW_GRP_WRITE	Yes/No	4	1746	1749	Is the group WRITE bit on for this file?
CSID_NEW_GRP_EXEC	Yes/No	4	1751	1754	Is the group EXECUTE bit on for this file?
CSID_NEW_OTH_READ	Yes/No	4	1756	1759	Is the other READ bit on for this file?
CSID_NEW_OTH_WRITE	Yes/No	4	1761	1764	Is the other WRITE bit on for this file?
CSID_NEW_OTH_EXEC	Yes/No	4	1766	1769	Is the other EXECUTE bit on for this file?
CSID_DFLT_PROCESS	Yes/No	4	1771	1774	Default z/OS UNIX security environment in effect.
CSID_UTK_NETW	Char	8	1776	1783	The port of entry network name.
CSID_X500_SUBJECT	Char	255	1785	2039	Subject's name associated with this event.
CSID_X500_ISSUER	Char	255	2041	2295	Issuer's name associated with this event.

Event Qualifiers for Clear SETID Records

The event qualifier that may be associated with clearing a file's SETID bits is shown in Table 72.

Table 72. Event Qualifiers for Clear SETID Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	S_ISUID, S_ISGID, and S_ISVTX changed. There are no failure cases for this event.

The Format of the EXEC SETUID/SETGID Record Extension

Table 73 describes the format of a record that is created by the execution of an EXEC SETUID or SETGID.

Table 73. Format of the EXEC with SETUID/SETGID Record Extension (Event Code 36)

Field Name	Type	Length	Position		Comments
			Start	End	
ESID_CLASS	Char	8	282	289	Class name.
ESID_USER_NAME	Char	20	291	310	The name associated with the user ID.
ESID_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
ESID_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
ESID_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
ESID_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
ESID_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
ESID_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
ESID_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
ESID_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
ESID_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
ESID_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
ESID_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
ESID_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
ESID_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
ESID_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
ESID_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
ESID_UTK_EXEENODE	Char	8	395	402	The execution node of the work.
ESID_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
ESID_UTK_SNODE	Char	8	413	420	The submitting node.
ESID_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
ESID_UTK_SPOE	Char	8	431	438	The port of entry.
ESID_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
ESID_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
ESID_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
ESID_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
ESID_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
ESID_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.

SMF Data Unload—IRRADU00

Table 73. Format of the EXEC with SETUID/SETGID Record Extension (Event Code 36) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
ESID_AUDIT_CODE	Char	11	494	504	Audit function code.
ESID_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
ESID_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
ESID_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
ESID_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
ESID_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
ESID_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
ESID_NEW_REAL_UID	Integer	10	572	581	New real z/OS UNIX user identifier (UID).
ESID_NEW_EFF_UID	Integer	10	583	592	New effective z/OS UNIX user identifier (UID).
ESID_NEW_SAVED_UID	Integer	10	594	603	New saved z/OS UNIX user identifier (UID).
ESID_NEW_REAL_GID	Integer	10	605	614	New real z/OS UNIX group identifier (GID).
ESID_NEW_EFF_GID	Integer	10	616	625	New effective z/OS UNIX group identifier (GID).
ESID_NEW_SAVED_GID	Integer	10	627	636	New saved z/OS UNIX group identifier (GID).
ESID_UID	Integer	10	638	647	The z/OS UNIX user identifier (UID) input parameter.
ESID_GID	Integer	10	649	658	The z/OS UNIX group identifier (GID) input parameter.
ESID_DFLT_PROCESS	Yes/No	4	660	663	Default z/OS UNIX security environment in effect.
ESID_UTK_NETW	Char	8	665	672	The port of entry network name.
ESID_X500_SUBJECT	Char	255	674	928	Subject's name associated with this event.
ESID_X500_ISSUER	Char	255	930	1184	Issuer's name associated with this event.

Event Qualifiers for EXEC with SETUID/SETGID Records

The event qualifier that may be associated with the execution of EXEC SETUID or EXEC SETGID is shown in Table 74.

Table 74. Event Qualifiers for EXEC with SETID/SETGID Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	z/OS UNIX user identifier (UID) or z/OS UNIX group identifier (GID) changed. There are no failure cases for this event.

The Format of the GETPSENT Record Extension

Table 75 describes the format of a record that is created by the GETPSENT service.

Table 75. Format of the GETPSENT Record Extension (Event Code 37)

Field Name	Type	Length	Position		Comments
			Start	End	
GPST_CLASS	Char	8	282	289	Class name.
GPST_USER_NAME	Char	20	291	310	The name associated with the user ID.
GPST_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
GPST_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
GPST_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?

Table 75. Format of the GETPSENT Record Extension (Event Code 37) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
GPST_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
GPST_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
GPST_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
GPST_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
GPST_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
GPST_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
GPST_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
GPST_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
GPST_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
GPST_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
GPST_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
GPST_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
GPST_UTK_EXECPNODE	Char	8	395	402	The execution node of the work.
GPST_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
GPST_UTK_SNODE	Char	8	413	420	The submitting node.
GPST_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
GPST_UTK_SPOE	Char	8	431	438	The port of entry.
GPST_UTK_SPCCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
GPST_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
GPST_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
GPST_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
GPST_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
GPST_APPC_LINK	Char	16	477	492	Key to link together APPC records.
GPST_AUDIT_CODE	Char	11	494	504	Audit function code.
GPST_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
GPST_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
GPST_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
GPST_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
GPST_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
GPST_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
GPST_TGT_REAL_UID	Integer	10	572	581	Target real z/OS UNIX user identifier (UID).
GPST_TGT_EFF_UID	Integer	10	583	592	Target effective z/OS UNIX user identifier (UID).
GPST_TGT_SAV_UID	Integer	10	594	603	Target saved z/OS UNIX user identifier (UID).
GPST_TGT_PID	Integer	10	605	614	Target process ID.
GPST_DFLT_PROCESS	Yes/No	4	616	619	Default z/OS UNIX security environment in effect.
GPST_UTK_NETW	Char	8	621	628	The port of entry network name.
GPST_X500_SUBJECT	Char	255	630	884	Subject's name associated with this event.
GPST_X500_ISSUER	Char	255	886	1140	Issuer's name associated with this event.

Event Qualifiers for the GETPSENT Record Extension

The event qualifiers that may be associated with the GETPSENT service are shown in Table 76 on page 176.

SMF Data Unload—IRRADU00

Table 76. Event Qualifiers for GETPSENT Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	GETPSENT was successful.
NOTAUTH	01	Not authorized to the specified process.

The Format of the Initialize z/OS UNIX Record Extension

Table 77 describes the format of a record that is created when a z/OS UNIX process is initialized.

Table 77. Format of the Initialize z/OS UNIX Process Record Extension (Event Code 38)

Field Name	Type	Length	Position		Comments
			Start	End	
IOEP_CLASS	Char	8	282	289	Class name.
IOEP_USER_NAME	Char	20	291	310	The name associated with the user ID.
IOEP_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
IOEP_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
IOEP_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
IOEP_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
IOEP_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
IOEP_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
IOEP_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
IOEP_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
IOEP_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
IOEP_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
IOEP_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
IOEP_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
IOEP_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
IOEP_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
IOEP_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
IOEP_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
IOEP_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
IOEP_UTK_SNODE	Char	8	413	420	The submitting node.
IOEP_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
IOEP_UTK_SPOE	Char	8	431	438	The port of entry.
IOEP_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
IOEP_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
IOEP_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
IOEP_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
IOEP_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
IOEP_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
IOEP_AUDIT_CODE	Char	11	494	504	Audit function code.
IOEP_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
IOEP_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).

Table 77. Format of the Initialize z/OS UNIX Process Record Extension (Event Code 38) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
IOEP_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
IOEP_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
IOEP_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
IOEP_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
IOEP_DFLT_PROCESS	Yes/No	4	572	575	Default z/OS UNIX security environment in effect.
IOEP_UTK_NETW	Char	8	577	584	The port of entry network name.
IOEP_X500_SUBJECT	Char	255	586	840	Subject's name associated with this event.
IOEP_X500_ISSUER	Char	255	842	1096	Issuer's name associated with this event.

Event Qualifiers for the Initialize z/OS UNIX Record Extension

The event qualifiers that may be associated with the initiation of a z/OS UNIX process are shown in Table 78.

Table 78. Event Qualifiers for Initialize z/OS UNIX Process Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Process successfully initialized.
NOTDFND	01	User not defined as a z/OS UNIX user. The OMVS segment or the user profile was missing.
NOUID	02	Incompletely defined user ID. There was no z/OS UNIX user identifier (UID) in profile.
NOGID	03	User's current group has no z/OS UNIX group identifier (GID).

The Format of the z/OS UNIX Process Completion Record

Table 79 describes the format of a record that is created when a z/OS UNIX process completes.

Table 79. Format of the z/OS UNIX Process Complete Record Extension (Event Code 39)

Field Name	Type	Length	Position		Comments
			Start	End	
TOEP_CLASS	Char	8	282	289	Class name.
TOEP_USER_NAME	Char	20	291	310	The name associated with the user ID.
TOEP_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
TOEP_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
TOEP_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
TOEP_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
TOEP_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
TOEP_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
TOEP_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
TOEP_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
TOEP_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
TOEP_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
TOEP_UTK_SESSTYPE	Char	8	362	369	The session type of this session.

SMF Data Unload—IRRADU00

Table 79. Format of the z/OS UNIX Process Complete Record Extension (Event Code 39) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
TOEP_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
TOEP_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
TOEP_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
TOEP_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
TOEP_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
TOEP_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
TOEP_UTK_SNODE	Char	8	413	420	The submitting node.
TOEP_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
TOEP_UTK_SPOE	Char	8	431	438	The port of entry.
TOEP_UTK_SPCCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
TOEP_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
TOEP_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
TOEP_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
TOEP_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
TOEP_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
TOEP_AUDIT_CODE	Char	11	494	504	Audit function code.
TOEP_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
TOEP_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
TOEP_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
TOEP_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
TOEP_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
TOEP_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
TOEP_DFLT_PROCESS	Yes/No	4	572	575	Default z/OS UNIX security environment in effect.
TOEP_UTK_NETW	Char	8	577	584	The port of entry network name.
TOEP_X500_SUBJECT	Char	255	586	840	Subject's name associated with this event.
TOEP_X500_ISSUER	Char	255	842	1096	Issuer's name associated with this event.

Event Qualifiers for the z/OS UNIX Process Complete Record Extension

The event qualifier that may be associated with the completion of a z/OS UNIX process is shown in Table 80.

Table 80. Event Qualifiers for z/OS UNIX Process Complete Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Process complete. There are no failure cases for this event.

The Format of the KILL Record Extension

Table 81 on page 179 describes the format of a record that is created by the termination with extreme prejudice of a process.

Table 81. Format of the KILL Process Record Extension (Event Code 40)

Field Name	Type	Length	Position		Comments
			Start	End	
KILL_CLASS	Char	8	282	289	Class name.
KILL_USER_NAME	Char	20	291	310	The name associated with the user ID.
KILL_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
KILL_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
KILL_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
KILL_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
KILL_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
KILL_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
KILL_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
KILL_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
KILL_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
KILL_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
KILL_UTK_SESTYPE	Char	8	362	369	The session type of this session.
KILL_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
KILL_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
KILL_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
KILL_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
KILL_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
KILL_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
KILL_UTK_SNODE	Char	8	413	420	The submitting node.
KILL_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
KILL_UTK_SPOE	Char	8	431	438	The port of entry.
KILL_UTK_SPCCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
KILL_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
KILL_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
KILL_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
KILL_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
KILL_APPC_LINK	Char	16	477	492	Key to link together APPC records.
KILL_AUDIT_CODE	Char	11	494	504	Audit function code.
KILL_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
KILL_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
KILL_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
KILL_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
KILL_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
KILL_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
KILL_TGT_REAL_UID	Integer	10	572	581	Target real z/OS UNIX user identifier (UID).
KILL_TGT_EFF_UID	Integer	10	583	592	Target effective z/OS UNIX user identifier (UID).
KILL_TGT_SAV_UID	Integer	10	594	603	Target saved z/OS UNIX user identifier (UID).
KILL_TGT_PID	Integer	10	605	614	Target process ID.
KILL_SIGNAL_CODE	Integer	10	616	625	Kill signal code.
KILL_DFLT_PROCESS	Yes/No	4	627	630	Default z/OS UNIX security environment in effect.
KILL_UTK_NETW	Char	8	632	639	The port of entry network name.

SMF Data Unload—IRRADU00

Table 81. Format of the KILL Process Record Extension (Event Code 40) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
KILL_X500_SUBJECT	Char	255	641	895	Subject's name associated with this event.
KILL_X500_ISSUER	Char	255	897	1151	Issuer's name associated with this event.

Event Qualifiers for the KILL Process Record Extension

The event qualifiers that may be associated with the killing of a process are shown in Table 82.

Table 82. Event Qualifiers for KILL Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Process terminated.
NOTAUTH	01	Not authorized to kill the specified process.

The Format of the LINK Record Extension

Table 83 describes the format of a record that is created by a LINK operation.

Table 83. Format of the LINK Record Extension (Event Code 41)

Field Name	Type	Length	Position		Comments
			Start	End	
LINK_CLASS	Char	8	282	289	Class name.
LINK_USER_NAME	Char	20	291	310	The name associated with the user ID.
LINK_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
LINK_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
LINK_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
LINK_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
LINK_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
LINK_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
LINK_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
LINK_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
LINK_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
LINK_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
LINK_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
LINK_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
LINK_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
LINK_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
LINK_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
LINK_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
LINK_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
LINK_UTK_SNODE	Char	8	413	420	The submitting node.
LINK_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
LINK_UTK_SPOE	Char	8	431	438	The port of entry.
LINK_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".

Table 83. Format of the LINK Record Extension (Event Code 41) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
LINK_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
LINK_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
LINK_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
LINK_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
LINK_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
LINK_AUDIT_CODE	Char	11	494	504	Audit function code.
LINK_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
LINK_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
LINK_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
LINK_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
LINK_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
LINK_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
LINK_PATH_NAME	Char	1023	572	1594	The requested path name.
LINK_FILE_ID	Char	32	1596	1627	File ID.
LINK_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
LINK_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
LINK_REQUEST_PATH2	Char	1023	1651	2673	Second requested path name.
LINK_PATH_TYPE	Char	4	2675	2678	Type of the requested path name. Valid values are "OLD" and "NEW".
LINK_FILEPOOL	Char	8	2680	2687	SFS filepool containing the BFS file.
LINK_FILESPACE	Char	8	2689	2696	SFS filespace containing the BFS filespace.
LINK_INODE	Integer	10	2698	2707	Inode (file serial number).
LINK_SCID	Integer	10	2709	2718	File SCID.
LINK_DCE_LINK	Char	16	2720	2735	Link to connect DCE records that originate from a single DCE request.
LINK_AUTH_TYPE	Char	13	2737	2749	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
LINK_DFLT_PROCESS	Yes/No	4	2751	2754	Default z/OS UNIX security environment in effect.
LINK_UTK_NETW	Char	8	2756	2763	The port of entry network name.
LINK_X500_SUBJECT	Char	255	2765	3019	Subject's name associated with this event.
LINK_X500_ISSUER	Char	255	3021	3275	Issuer's name associated with this event.

Event Qualifiers for LINK Records

The event qualifier that may be associated with a LINK event is shown in Table 84.

Table 84. Event Qualifiers for LINK Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	New link created. There are no failure cases for this event.

The Format of the MKDIR Record Extension

Table 85 describes the format of a record that is created by making a directory.

Table 85. Format of the MKDIR Record Extension (Event Code 42)

Field Name	Type	Length	Position		Comments
			Start	End	
MDIR_CLASS	Char	8	282	289	Class name.
MDIR_USER_NAME	Char	20	291	310	The name associated with the user ID.
MDIR_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
MDIR_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
MDIR_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
MDIR_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
MDIR_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
MDIR_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
MDIR_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
MDIR_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
MDIR_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
MDIR_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
MDIR_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
MDIR_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
MDIR_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
MDIR_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
MDIR_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
MDIR_UTK_EXEENODE	Char	8	395	402	The execution node of the work.
MDIR_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
MDIR_UTK_SNODE	Char	8	413	420	The submitting node.
MDIR_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
MDIR_UTK_SPOE	Char	8	431	438	The port of entry.
MDIR_UTK_SPCCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
MDIR_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
MDIR_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
MDIR_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
MDIR_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
MDIR_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
MDIR_AUDIT_CODE	Char	11	494	504	Audit function code.
MDIR_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
MDIR_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
MDIR_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
MDIR_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
MDIR_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
MDIR_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
MDIR_PATH_NAME	Char	1023	572	1594	The requested path name.
MDIR_FILE_ID	Char	32	1596	1627	File ID.
MDIR_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.

Table 85. Format of the MKDIR Record Extension (Event Code 42) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
MDIR_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
MDIR_OLD_S_ISGID	Yes/No	4	1651	1654	Was the S_ISGID bit requested on for this file?
MDIR_OLD_S_ISUID	Yes/No	4	1656	1659	Was the S_ISUID bit requested on for this file?
MDIR_OLD_S_ISVTX	Yes/No	4	1661	1664	Was the S_ISVTX bit requested on for this file?
MDIR_OLD_OWN_READ	Yes/No	4	1666	1669	Was the owner READ bit on for this file?
MDIR_OLD_OWN_WRITE	Yes/No	4	1671	1674	Was the owner WRITE bit on for this file?
MDIR_OLD_OWN_EXEC	Yes/No	4	1676	1679	Was the owner EXECUTE bit on for this file?
MDIR_OLD_GRP_READ	Yes/No	4	1681	1684	Was the group READ bit on for this file?
MDIR_OLD_GRP_WRITE	Yes/No	4	1686	1689	Was the group WRITE bit on for this file?
MDIR_OLD_GRP_EXEC	Yes/No	4	1691	1694	Was the group EXECUTE bit on for this file?
MDIR_OLD_OTH_READ	Yes/No	4	1696	1699	Was the other READ bit on for this file?
MDIR_OLD_OTH_WRITE	Yes/No	4	1701	1704	Was the other WRITE bit on for this file?
MDIR_OLD_OTH_EXEC	Yes/No	4	1706	1709	Was the other EXECUTE bit on for this file?
MDIR_NEW_S_ISGID	Yes/No	4	1711	1714	Is the S_ISGID bit requested on for this file?
MDIR_NEW_S_ISUID	Yes/No	4	1716	1719	Is the S_ISUID bit requested on for this file?
MDIR_NEW_S_ISVTX	Yes/No	4	1721	1724	Is the S_ISVTX bit requested on for this file?
MDIR_NEW_OWN_READ	Yes/No	4	1726	1729	Is the owner READ bit on for this file?
MDIR_NEW_OWN_WRITE	Yes/No	4	1731	1734	Is the owner WRITE bit on for this file?
MDIR_NEW_OWN_EXEC	Yes/No	4	1736	1739	Is the owner EXECUTE bit on for this file?
MDIR_NEW_GRP_READ	Yes/No	4	1741	1744	Is the group READ bit on for this file?
MDIR_NEW_GRP_WRITE	Yes/No	4	1746	1749	Is the group WRITE bit on for this file?
MDIR_NEW_GRP_EXEC	Yes/No	4	1751	1754	Is the group EXECUTE bit on for this file?
MDIR_NEW_OTH_READ	Yes/No	4	1756	1759	Is the other READ bit on for this file?
MDIR_NEW_OTH_WRITE	Yes/No	4	1761	1764	Is the other WRITE bit on for this file?
MDIR_NEW_OTH_EXEC	Yes/No	4	1766	1769	Is the other EXECUTE bit on for this file?
MDIR_UNEW_READ	Char	8	1771	1778	What are the new user audit options for READ actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
MDIR_UNEW_WRITE	Char	8	1780	1787	What are the new user audit options for WRITE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
MDIR_UNEW_EXEC	Char	8	1789	1796	What are the new user audit options for EXECUTE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
MDIR_ANEW_READ	Char	8	1798	1805	What are the new auditor audit options for READ actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
MDIR_ANEW_WRITE	Char	8	1807	1814	What are the new auditor audit options for WRITE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
MDIR_ANEW_EXEC	Char	8	1816	1823	What are the new auditor audit options for EXECUTE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
MDIR_REQ_S_ISGID	Yes/No	4	1825	1828	Was the S_ISGID bit requested on for this file?
MDIR_REQ_S_ISUID	Yes/No	4	1830	1833	Was the S_ISUID bit requested on for this file?
MDIR_REQ_S_ISVTX	Yes/No	4	1835	1838	Was the S_ISVTX bit requested on for this file?

SMF Data Unload—IRRADU00

Table 85. Format of the MKDIR Record Extension (Event Code 42) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
MDIR_REQ_OWN_READ	Yes/No	4	1840	1843	Was the owner READ bit requested on for this file?
MDIR_REQ_OWN_WRITE	Yes/No	4	1845	1848	Was the owner WRITE bit requested on for this file?
MDIR_REQ_OWN_EXEC	Yes/No	4	1850	1853	Was the owner EXECUTE bit requested on for this file?
MDIR_REQ_GRP_READ	Yes/No	4	1855	1858	Was the group READ bit requested on for this file?
MDIR_REQ_GRP_WRITE	Yes/No	4	1860	1863	Was the group WRITE bit requested on for this file?
MDIR_REQ_GRP_EXEC	Yes/No	4	1865	1868	Was the group EXECUTE bit requested on for this file?
MDIR_REQ_OTH_READ	Yes/No	4	1870	1873	Was the other READ bit requested on for this file?
MDIR_REQ_OTH_WRITE	Yes/No	4	1875	1878	Was the other WRITE bit requested on for this file?
MDIR_REQ_OTH_EXEC	Yes/No	4	1880	1883	Was the other EXECUTE bit requested on for this file?
MDIR_FILEPOOL	Char	8	1885	1892	SFS filepool containing the BFS file.
MDIR_FILESPACE	Char	8	1894	1901	SFS filespace containing the BFS file.
MDIR_INODE	Integer	10	1903	1912	Inode (file serial number).
MDIR_SCID	Integer	10	1914	1923	File SCID.
MDIR_DFLT_PROCESS	Yes/No	4	1925	1928	Default z/OS UNIX security environment in effect.
MDIR_UTK_NETW	Char	8	1930	1937	The port of entry network name.
MDIR_X500_SUBJECT	Char	255	1939	2193	Subject's name associated with this event.
MDIR_X500_ISSUER	Char	255	2195	2449	Issuer's name associated with this event.

Event Qualifiers for MKDIR Records

The event qualifier that may be associated with making a directory is shown in Table 86.

Table 86. Event Qualifiers for MKDIR Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Directory created. There are no failure cases for this event.

The Format of the MKNOD Record Extension

Table 87 describes the format of a record that is created by making a node.

Table 87. Format of the MKNOD Extension (Event Code 43)

Field Name	Type	Length	Position		Comments
			Start	End	
MNOD_CLASS	Char	8	282	289	Class name.
MNOD_USER_NAME	Char	20	291	310	The name associated with the user ID.
MNOD_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?

Table 87. Format of the MKNOD Extension (Event Code 43) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
MNOD_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
MNOD_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
MNOD_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
MNOD_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
MNOD_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
MNOD_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
MNOD_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
MNOD_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
MNOD_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
MNOD_UTK_SESTYPE	Char	8	362	369	The session type of this session.
MNOD_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
MNOD_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
MNOD_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
MNOD_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
MNOD_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
MNOD_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
MNOD_UTK_SNODE	Char	8	413	420	The submitting node.
MNOD_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
MNOD_UTK_SPOE	Char	8	431	438	The port of entry.
MNOD_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
MNOD_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
MNOD_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
MNOD_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
MNOD_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
MNOD_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
MNOD_AUDIT_CODE	Char	11	494	504	Audit function code.
MNOD_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
MNOD_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
MNOD_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
MNOD_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
MNOD_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
MNOD_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
MNOD_PATH_NAME	Char	1023	572	1594	The requested path name.
MNOD_FILE_ID	Char	32	1596	1627	File ID.
MNOD_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
MNOD_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
MNOD_OLD_S_ISGID	Yes/No	4	1651	1654	Was the S_ISGID bit requested on for this file?
MNOD_OLD_S_ISUID	Yes/No	4	1656	1659	Was the S_ISUID bit requested on for this file?
MNOD_OLD_S_ISVTX	Yes/No	4	1661	1664	Was the S_ISVTX bit requested on for this file?
MNOD_OLD_OWN_READ	Yes/No	4	1666	1669	Was the owner READ bit on for this file?

SMF Data Unload—IRRADU00

Table 87. Format of the MKNOD Extension (Event Code 43) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
MNOD_OLD_OWN_WRITE	Yes/No	4	1671	1674	Was the owner WRITE bit on for this file?
MNOD_OLD_OWN_EXEC	Yes/No	4	1676	1679	Was the owner EXECUTE bit on for this file?
MNOD_OLD_GRP_READ	Yes/No	4	1681	1684	Was the group READ bit on for this file?
MNOD_OLD_GRP_WRITE	Yes/No	4	1686	1689	Was the group WRITE bit on for this file?
MNOD_OLD_GRP_EXEC	Yes/No	4	1691	1694	Was the group EXECUTE bit on for this file?
MNOD_OLD_OTH_READ	Yes/No	4	1696	1699	Was the other READ bit on for this file?
MNOD_OLD_OTH_WRITE	Yes/No	4	1701	1704	Was the other WRITE bit on for this file?
MNOD_OLD_OTH_EXEC	Yes/No	4	1706	1709	Was the other EXECUTE bit on for this file?
MNOD_NEW_S_ISGID	Yes/No	4	1711	1714	Is the S_ISGID bit requested on for this file?
MNOD_NEW_S_ISUID	Yes/No	4	1716	1719	Is the S_ISUID bit requested on for this file?
MNOD_NEW_S_ISVTX	Yes/No	4	1721	1724	Is the S_ISVTX bit requested on for this file?
MNOD_NEW_OWN_READ	Yes/No	4	1726	1729	Is the owner READ bit on for this file?
MNOD_NEW_OWN_WRITE	Yes/No	4	1731	1734	Is the owner WRITE bit on for this file?
MNOD_NEW_OWN_EXEC	Yes/No	4	1736	1739	Is the owner EXECUTE bit on for this file?
MNOD_NEW_GRP_READ	Yes/No	4	1741	1744	Is the group READ bit on for this file?
MNOD_NEW_GRP_WRITE	Yes/No	4	1746	1749	Is the group WRITE bit on for this file?
MNOD_NEW_GRP_EXEC	Yes/No	4	1751	1754	Is the group EXECUTE bit on for this file?
MNOD_NEW_OTH_READ	Yes/No	4	1756	1759	Is the other READ bit on for this file?
MNOD_NEW_OTH_WRITE	Yes/No	4	1761	1764	Is the other WRITE bit on for this file?
MNOD_NEW_OTH_EXEC	Yes/No	4	1766	1769	Is the other EXECUTE bit on for this file?
MNOD_UNEW_READ	Char	8	1771	1778	What are the new user audit options for READ actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
MNOD_UNEW_WRITE	Char	8	1780	1787	What are the new user audit options for WRITE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
MNOD_UNEW_EXEC	Char	8	1789	1796	What are the new user audit options for EXECUTE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
MNOD_ANEW_READ	Char	8	1798	1805	What are the new auditor audit options for READ actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
MNOD_ANEW_WRITE	Char	8	1807	1814	What are the new auditor audit options for WRITE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
MNOD_ANEW_EXEC	Char	8	1816	1823	What are the new auditor audit options for EXECUTE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
MNOD_REQ_S_ISGID	Yes/No	4	1825	1828	Was the S_ISGID bit requested on for this file?
MNOD_REQ_S_ISUID	Yes/No	4	1830	1833	Was the S_ISUID bit requested on for this file?
MNOD_REQ_S_ISVTX	Yes/No	4	1835	1838	Was the S_ISVTX bit requested on for this file?
MNOD_REQ_OWN_READ	Yes/No	4	1840	1843	Was the owner READ bit requested on for this file?
MNOD_REQ_OWN_WRITE	Yes/No	4	1845	1848	Was the owner WRITE bit requested on for this file?
MNOD_REQ_OWN_EXEC	Yes/No	4	1850	1853	Was the owner EXECUTE bit requested on for this file?
MNOD_REQ_GRP_READ	Yes/No	4	1855	1858	Was the group READ bit requested on for this file?

Table 87. Format of the MKNOD Extension (Event Code 43) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
MNOD_REQ_GRP_WRITE	Yes/No	4	1860	1863	Was the group WRITE bit requested on for this file?
MNOD_REQ_GRP_EXEC	Yes/No	4	1865	1868	Was the group EXECUTE bit requested on for this file?
MNOD_REQ_OTH_READ	Yes/No	4	1870	1873	Was the other READ bit requested on for this file?
MNOD_REQ_OTH_WRITE	Yes/No	4	1875	1878	Was the other WRITE bit requested on for this file?
MNOD_REQ_OTH_EXEC	Yes/No	4	1880	1883	Was the other EXECUTE bit requested on for this file?
MNOD_FILEPOOL	Char	8	1885	1892	SFS filepool containing the BFS file.
MNOD_FILESPACE	Char	8	1894	1901	SFS filespace containing the BFS file.
MNOD_INODE	Integer	10	1903	1912	Inode (file serial number).
MNOD_SCID	Integer	10	1914	1923	File SCID.
MNOD_DFLT_PROCESS	Yes/No	4	1925	1928	Default z/OS UNIX security environment in effect.
MNOD_UTK_NETW	Char	8	1930	1937	The port of entry network name.
MNOD_X500_SUBJECT	Char	255	1939	2193	Subject's name associated with this event.
MNOD_X500_ISSUER	Char	255	2195	2449	Issuer's name associated with this event.

Event Qualifiers for MKNOD Records

The event qualifier that may be associated with making a node is shown in Table 88.

Table 88. Event Qualifiers for MKNOD Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Node created. There are no failure cases for this event.

The Format of the Mount File System Record Extension

Table 89 describes the format of a record that is created by mounting a file system.

Table 89. Format of the Mount File System Record Extension (Event Code 44)

Field Name	Type	Length	Position		Comments
			Start	End	
MFS_CLASS	Char	8	282	289	Class name.
MFS_USER_NAME	Char	20	291	310	The name associated with the user ID.
MFS_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
MFS_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
MFS_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
MFS_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
MFS_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
MFS_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
MFS_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
MFS_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?

SMF Data Unload—IRRADU00

Table 89. Format of the Mount File System Record Extension (Event Code 44) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
MFS_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
MFS_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
MFS_UTK_SESTYPE	Char	8	362	369	The session type of this session.
MFS_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
MFS_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
MFS_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
MFS_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
MFS_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
MFS_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
MFS_UTK_SNODE	Char	8	413	420	The submitting node.
MFS_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
MFS_UTK_SPOE	Char	8	431	438	The port of entry.
MFS_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
MFS_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
MFS_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
MFS_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
MFS_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
MFS_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
MFS_AUDIT_CODE	Char	11	494	504	Audit function code.
MFS_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
MFS_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
MFS_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
MFS_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
MFS_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
MFS_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
MFS_PATH_NAME	Char	1023	572	1594	The requested path name.
MFS_FILE_ID	Char	32	1596	1627	File ID.
MFS_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
MFS_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
MFS_HFS_DS_NAME	Char	44	1651	1694	HFS data set name for the mounted file system.
MFS_DCE_LINK	Char	16	1696	1711	Link to connect DCE records that originate from a single DCE request.
MFS_AUTH_TYPE	Char	13	1713	1725	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
MFS_DFLT_PROCESS	Yes/No	4	1727	1730	Default z/OS UNIX security environment in effect.
MFS_UTK_NETW	Char	8	1732	1739	The port of entry network name.
MFS_X500_SUBJECT	Char	255	1741	1995	Subject's name associated with this event.
MFS_X500_ISSUER	Char	255	1997	2251	Issuer's name associated with this event.

Event Qualifiers for Mount File System Records

The event qualifier that may be associated with the mounting of a file system event is shown in Table 90.

Table 90. Event Qualifiers for Mount File System Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	File system mounted. There are no failure cases for this event.

The Format of the OPENFILE Record Extension

Table 91 describes the format of a record that is created by opening a file.

Table 91. Format of the OPENFILE Extension (Event Code 45)

Field Name	Type	Length	Position		Comments
			Start	End	
OPEN_CLASS	Char	8	282	289	Class name.
OPEN_USER_NAME	Char	20	291	310	The name associated with the user ID.
OPEN_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
OPEN_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
OPEN_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
OPEN_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
OPEN_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
OPEN_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
OPEN_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
OPEN_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
OPEN_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
OPEN_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
OPEN_UTK_SESTYPE	Char	8	362	369	The session type of this session.
OPEN_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
OPEN_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
OPEN_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
OPEN_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
OPEN_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
OPEN_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
OPEN_UTK_SNODE	Char	8	413	420	The submitting node.
OPEN_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
OPEN_UTK_SPOE	Char	8	431	438	The port of entry.
OPEN_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
OPEN_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
OPEN_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
OPEN_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
OPEN_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
OPEN_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
OPEN_AUDIT_CODE	Char	11	494	504	Audit function code.

SMF Data Unload—IRRADU00

Table 91. Format of the OPENFILE Extension (Event Code 45) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
OPEN_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
OPEN_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
OPEN_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
OPEN_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
OPEN_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
OPEN_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
OPEN_PATH_NAME	Char	1023	572	1594	The requested path name.
OPEN_FILE_ID	Char	32	1596	1627	File ID.
OPEN_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
OPEN_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
OPEN_OLD_S_ISGID	Yes/No	4	1651	1654	Was the S_ISGID bit requested on for this file?
OPEN_OLD_S_ISUID	Yes/No	4	1656	1659	Was the S_ISUID bit requested on for this file?
OPEN_OLD_S_ISVTX	Yes/No	4	1661	1664	Was the S_ISVTX bit requested on for this file?
OPEN_OLD_OWN_READ	Yes/No	4	1666	1669	Was the owner READ bit on for this file?
OPEN_OLD_OWN_WRITE	Yes/No	4	1671	1674	Was the owner WRITE bit on for this file?
OPEN_OLD_OWN_EXEC	Yes/No	4	1676	1679	Was the owner EXECUTE bit on for this file?
OPEN_OLD_GRP_READ	Yes/No	4	1681	1684	Was the group READ bit on for this file?
OPEN_OLD_GRP_WRITE	Yes/No	4	1686	1689	Was the group WRITE bit on for this file?
OPEN_OLD_GRP_EXEC	Yes/No	4	1691	1694	Was the group EXECUTE bit on for this file?
OPEN_OLD_OTH_READ	Yes/No	4	1696	1699	Was the other READ bit on for this file?
OPEN_OLD_OTH_WRITE	Yes/No	4	1701	1704	Was the other WRITE bit on for this file?
OPEN_OLD_OTH_EXEC	Yes/No	4	1706	1709	Was the other EXECUTE bit on for this file?
OPEN_NEW_S_ISGID	Yes/No	4	1711	1714	Is the S_ISGID bit requested on for this file?
OPEN_NEW_S_ISUID	Yes/No	4	1716	1719	Is the S_ISUID bit requested on for this file?
OPEN_NEW_S_ISVTX	Yes/No	4	1721	1724	Is the S_ISVTX bit requested on for this file?
OPEN_NEW_OWN_READ	Yes/No	4	1726	1729	Is the owner READ bit on for this file?
OPEN_NEW_OWN_WRITE	Yes/No	4	1731	1734	Is the owner WRITE bit on for this file?
OPEN_NEW_OWN_EXEC	Yes/No	4	1736	1739	Is the owner EXECUTE bit on for this file?
OPEN_NEW_GRP_READ	Yes/No	4	1741	1744	Is the group READ bit on for this file?
OPEN_NEW_GRP_WRITE	Yes/No	4	1746	1749	Is the group WRITE bit on for this file?
OPEN_NEW_GRP_EXEC	Yes/No	4	1751	1754	Is the group EXECUTE bit on for this file?
OPEN_NEW_OTH_READ	Yes/No	4	1756	1759	Is the other READ bit on for this file?
OPEN_NEW_OTH_WRITE	Yes/No	4	1761	1764	Is the other WRITE bit on for this file?
OPEN_NEW_OTH_EXEC	Yes/No	4	1766	1769	Is the other EXECUTE bit on for this file?
OPEN_UNEW_READ	Char	8	1771	1778	What are the new user audit options for READ actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
OPEN_UNEW_WRITE	Char	8	1780	1787	What are the new user audit options for WRITE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
OPEN_UNEW_EXEC	Char	8	1789	1796	What are the new user audit options for EXECUTE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".

Table 91. Format of the OPENFILE Extension (Event Code 45) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
OPEN_ANEW_READ	Char	8	1798	1805	What are the new auditor audit options for READ actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
OPEN_ANEW_WRITE	Char	8	1807	1814	What are the new auditor audit options for WRITE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
OPEN_ANEW_EXEC	Char	8	1816	1823	What are the new auditor audit options for EXECUTE actions? Valid values are "NONE", "SUCCESS", "FAIL", and "ALL".
OPEN_REQ_S_ISGID	Yes/No	4	1825	1828	Was the S_ISGID bit requested on for this file?
OPEN_REQ_S_ISUID	Yes/No	4	1830	1833	Was the S_ISUID bit requested on for this file?
OPEN_REQ_S_ISVTX	Yes/No	4	1835	1838	Was the S_ISVTX bit requested on for this file?
OPEN_REQ_OWN_READ	Yes/No	4	1840	1843	Was the owner READ bit requested on for this file?
OPEN_REQ_OWN_WRITE	Yes/No	4	1845	1848	Was the owner WRITE bit requested on for this file?
OPEN_REQ_OWN_EXEC	Yes/No	4	1850	1853	Was the owner EXECUTE bit requested on for this file?
OPEN_REQ_GRP_READ	Yes/No	4	1855	1858	Was the group READ bit requested on for this file?
OPEN_REQ_GRP_WRITE	Yes/No	4	1860	1863	Was the group WRITE bit requested on for this file?
OPEN_REQ_GRP_EXEC	Yes/No	4	1865	1868	Was the group EXECUTE bit requested on for this file?
OPEN_REQ_OTH_READ	Yes/No	4	1870	1873	Was the other READ bit requested on for this file?
OPEN_REQ_OTH_WRITE	Yes/No	4	1875	1878	Was the other WRITE bit requested on for this file?
OPEN_REQ_OTH_EXEC	Yes/No	4	1880	1883	Was the other EXECUTE bit requested on for this file?
OPEN_FILEPOOL	Char	8	1885	1892	SFS filepool containing the BFS file.
OPEN_FILESPACE	Char	8	1894	1901	SFS filespace containing the BFS file.
OPEN_INODE	Integer	10	1903	1912	Inode (file serial number).
OPEN_SCID	Integer	10	1914	1923	File SCID.
OPEN_DFLT_PROCESS	Yes/No	4	1925	1928	Default z/OS UNIX security environment in effect.
OPEN_UTK_NETW	Char	8	1930	1937	The port of entry network name.
OPEN_X500_SUBJECT	Char	255	1939	2193	Subject's name associated with this event.
OPEN_X500_ISSUER	Char	255	2195	2449	Issuer's name associated with this event.

Event Qualifiers for OPENFILE Records

The event qualifier that may be associated with making a node is shown in Table 92.

Table 92. Event Qualifiers for OPENFILE Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	File created. There are no failure cases for this event.

The Format of the PTRACE Record Extension

Table 93 describes the format of a record that is created by the tracing of a process.

Table 93. Format of the PTRACE Record Extension (Event Code 46)

Field Name	Type	Length	Position		Comments
			Start	End	
PTRC_CLASS	Char	8	282	289	Class name.
PTRC_USER_NAME	Char	20	291	310	The name associated with the user ID.
PTRC_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
PTRC_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
PTRC_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
PTRC_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
PTRC_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
PTRC_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
PTRC_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
PTRC_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
PTRC_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
PTRC_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
PTRC_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
PTRC_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
PTRC_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
PTRC_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
PTRC_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
PTRC_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
PTRC_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
PTRC_UTK_SNODE	Char	8	413	420	The submitting node.
PTRC_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
PTRC_UTK_SPOE	Char	8	431	438	The port of entry.
PTRC_UTK_SPCCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
PTRC_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
PTRC_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
PTRC_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
PTRC_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
PTRC_APPC_LINK	Char	16	477	492	Key to link together APPC records.
PTRC_AUDIT_CODE	Char	11	494	504	Audit function code.
PTRC_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
PTRC_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
PTRC_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
PTRC_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
PTRC_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
PTRC_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
PTRC_TGT_REAL_UID	Integer	10	572	581	Target real z/OS UNIX user identifier (UID).
PTRC_TGT_EFF_UID	Integer	10	583	592	Target effective z/OS UNIX user identifier (UID).
PTRC_TGT_SAVED_UID	Integer	10	594	603	Target saved z/OS UNIX user identifier (UID).

Table 93. Format of the PTRACE Record Extension (Event Code 46) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
PTRC_TGT_REAL_GID	Integer	10	605	614	Target real z/OS UNIX group identifier (GID).
PTRC_TGT_EFF_GID	Integer	10	616	625	Target effective z/OS UNIX group identifier (GID).
PTRC_TGT_SAVED_GID	Integer	10	627	636	Target saved z/OS UNIX group identifier (GID).
PTRC_TGT_PID	Integer	10	638	647	Target process ID.
PTRC_DFLT_PROCESS	Yes/No	4	649	652	Default z/OS UNIX security environment in effect.
PTRC_UTK_NETW	Char	8	654	661	The port of entry network name.
PTRC_X500_SUBJECT	Char	255	663	917	Subject's name associated with this event.
PTRC_X500_ISSUER	Char	255	919	1173	Issuer's name associated with this event.

Event Qualifiers for the PTRACE Process Record Extension

The event qualifiers that may be associated with the tracing of a process are shown in Table 94.

Table 94. Event Qualifiers for PTRACE Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Access allowed.
NOTAUTH	01	Not authorized to trace the specified process.

The Format of the Rename File Record Extension

Table 83 on page 180 describes the format of a record that is created by a rename operation.

Table 95. Format of the Rename File Record Extension (Event Code 47)

Field Name	Type	Length	Position		Comments
			Start	End	
RENF_CLASS	Char	8	282	289	Class name.
RENF_USER_NAME	Char	20	291	310	The name associated with the user ID.
RENF_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
RENF_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
RENF_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
RENF_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
RENF_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
RENF_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
RENF_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
RENF_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
RENF_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
RENF_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
RENF_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
RENF_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
RENF_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
RENF_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
RENF_UTK_SECL	Char	8	386	393	The SECLABEL of the user.

SMF Data Unload—IRRADU00

Table 95. Format of the Rename File Record Extension (Event Code 47) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
RENF_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
RENF_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
RENF_UTK_SNODE	Char	8	413	420	The submitting node.
RENF_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
RENF_UTK_SPOE	Char	8	431	438	The port of entry.
RENF_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
RENF_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
RENF_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
RENF_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
RENF_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
RENF_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
RENF_AUDIT_CODE	Char	11	494	504	Audit function code.
RENF_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
RENF_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
RENF_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
RENF_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
RENF_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
RENF_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
RENF_PATH_NAME	Char	1023	572	1594	The requested path name.
RENF_FILE_ID	Char	32	1596	1627	File ID.
RENF_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
RENF_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
RENF_PATH2	Char	1023	1651	2673	Second requested path name.
RENF_FILE_ID2	Char	32	2675	2706	Second requested file ID.
RENF_OWNER_UID	Integer	10	2708	2717	z/OS UNIX user identifier (UID) of the owner of the deleted file.
RENF_OWNER_GID	Integer	10	2719	2728	z/OS UNIX group identifier (GID) of the owner of the deleted file.
RENF_PATH_TYPE	Char	4	2730	2733	Type of the requested path name. Valid values are "OLD" and "NEW".
RENF_LAST_DELETED	Yes/No	4	2735	2738	Was the last link deleted?
RENF_FILEPOOL	Char	8	2740	2747	SFS filepool containing the BFS file.
RENF_FILESPACE	Char	8	2749	2756	SFS filespace containing the BFS file.
RENF_INODE	Integer	10	2758	2767	Inode (file serial number).
RENF_SCID	Integer	10	2769	2778	File SCID.
RENF_FILEPOOL2	Char	8	2780	2787	SFS filepool containing the second BFS file.
RENF_FILESPACE2	Char	8	2789	2796	SFS filespace containing the second BFS file.
RENF_INODE2	Integer	10	2798	2807	Second Inode (file serial number).
RENF_SCID2	Integer	10	2809	2818	Second file SCID.
RENF_DCE_LINK	Char	16	2820	2835	Link to connect DCE records that originate from a single DCE request.

Table 95. Format of the Rename File Record Extension (Event Code 47) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
RENF_AUTH_TYPE	Char	13	2837	2849	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
RENF_DFLT_PROCESS	Yes/No	4	2851	2854	Default z/OS UNIX security environment in effect.
RENF_UTK_NETW	Char	8	2856	2863	The port of entry network name.
RENF_X500_SUBJECT	Char	255	2865	3119	Subject's name associated with this event.
RENF_X500_ISSUER	Char	255	3121	3375	Issuer's name associated with this event.

Event Qualifiers for Rename File Records

The event qualifier that may be associated with a file rename event is shown in Table 96.

Table 96. Event Qualifiers for Rename File Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	File renamed. There are no failure cases for this event.

The Format of the RMDIR Record Extension

Table 97 describes the format of a record that is created by removing a directory.

Table 97. Format of the RMDIR Record Extension (Event Code 48)

Field Name	Type	Length	Position		Comments
			Start	End	
RDIR_CLASS	Char	8	282	289	Class name.
RDIR_USER_NAME	Char	20	291	310	The name associated with the user ID.
RDIR_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
RDIR_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
RDIR_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
RDIR_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
RDIR_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
RDIR_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
RDIR_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
RDIR_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
RDIR_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
RDIR_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
RDIR_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
RDIR_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
RDIR_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
RDIR_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
RDIR_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
RDIR_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
RDIR_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
RDIR_UTK_SNODE	Char	8	413	420	The submitting node.

SMF Data Unload—IRRADU00

Table 97. Format of the RMDIR Record Extension (Event Code 48) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
RDIR_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
RDIR_UTK_SPOE	Char	8	431	438	The port of entry.
RDIR_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
RDIR_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
RDIR_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
RDIR_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
RDIR_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
RDIR_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
RDIR_AUDIT_CODE	Char	11	494	504	Audit function code.
RDIR_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
RDIR_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
RDIR_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
RDIR_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
RDIR_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
RDIR_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
RDIR_PATH_NAME	Char	1023	572	1594	The requested path name.
RDIR_FILE_ID	Char	32	1596	1627	File ID.
RDIR_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
RDIR_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
RDIR_FILEPOOL	Char	8	1651	1658	SFS filepool containing the BFS file.
RDIR_FILESPACE	Char	8	1660	1667	SFS filespace containing the BFS file.
RDIR_INODE	Integer	10	1669	1678	Inode (file serial number).
RDIR_SCID	Integer	10	1680	1689	File SCID.
RDIR_DCE_LINK	Char	16	1691	1706	Link to connect DCE records that originate from a single DCE request.
RDIR_AUTH_TYPE	Char	13	1708	1720	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
RDIR_DFLT_PROCESS	Yes/No	4	1722	1725	Default z/OS UNIX security environment in effect.
RDIR_UTK_NETW	Char	8	1727	1734	The port of entry network name.
RDIR_X500_SUBJECT	Char	255	1736	1990	Subject's name associated with this event.
RDIR_X500_ISSUER	Char	255	1992	2246	Issuer's name associated with this event.

Event Qualifiers for RMDIR Records

The event qualifier that may be associated with removing a directory is shown in Table 98.

Table 98. Event Qualifiers for RMDIR Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Directory removed. There are no failure cases for this event.

The Format of the SETEGID (SET Effective z/OS UNIX Group Identifier (GID) Record Extension

Table 99 describes the format of a record that is created by the setting of an effective z/OS UNIX group identifier (GID).

Table 99. Format of the SETEGID Record Extension (Event Code 49)

Field Name	Type	Length	Position		Comments
			Start	End	
SEGI_CLASS	Char	8	282	289	Class name.
SEGI_USER_NAME	Char	20	291	310	The name associated with the user ID.
SEGI_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
SEGI_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
SEGI_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
SEGI_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
SEGI_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
SEGI_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
SEGI_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
SEGI_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
SEGI_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
SEGI_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
SEGI_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
SEGI_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
SEGI_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
SEGI_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
SEGI_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
SEGI_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
SEGI_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
SEGI_UTK_SNODE	Char	8	413	420	The submitting node.
SEGI_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
SEGI_UTK_SPOE	Char	8	431	438	The port of entry.
SEGI_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
SEGI_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
SEGI_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
SEGI_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
SEGI_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
SEGI_APPC_LINK	Char	16	477	492	Key to link together APPC records.
SEGI_AUDIT_CODE	Char	11	494	504	Audit function code.
SEGI_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
SEGI_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
SEGI_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
SEGI_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
SEGI_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
SEGI_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
SEGI_NEW_REAL_GID	Integer	10	572	581	New real z/OS UNIX group identifier (GID).
SEGI_NEW_EFF_GID	Integer	10	583	592	New effective z/OS UNIX group identifier (GID).

SMF Data Unload—IRRADU00

Table 99. Format of the SETEGID Record Extension (Event Code 49) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
SEGI_NEW_SAVED_GID	Integer	10	594	603	New saved z/OS UNIX group identifier (GID).
SEGI_GID	Integer	10	605	614	The z/OS UNIX group identifier (GID) input parameter.
SEGI_DFLT_PROCESS	Yes/No	4	616	619	Default z/OS UNIX security environment in effect.
SEGI_UTK_NETW	Char	8	621	628	The port of entry network name.
SEGI_X500_SUBJECT	Char	255	630	884	Subject's name associated with this event.
SEGI_X500_ISSUER	Char	255	886	1140	Issuer's name associated with this event.

Event Qualifiers for the SETEGID Record Extension

The event qualifiers that may be associated with setting the effective z/OS UNIX group identifier (GID) are shown in Table 100.

Table 100. Event Qualifiers for SETEGID Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Successful change of effective z/OS UNIX group identifier (GID).
NOTAUTH	01	Not authorized to set the effective z/OS UNIX group identifier (GID).

The Format of the SETEUID (SET Effective z/OS UNIX User Identifier (UID) Record Extension

Table 101 describes the format of a record that is created by the setting of an effective z/OS UNIX user identifier (UID).

Table 101. Format of the SETEUID Record Extension (Event Code 50)

Field Name	Type	Length	Position		Comments
			Start	End	
SEUI_CLASS	Char	8	282	289	Class name.
SEUI_USER_NAME	Char	20	291	310	The name associated with the user ID.
SEUI_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
SEUI_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
SEUI_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
SEUI_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
SEUI_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
SEUI_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
SEUI_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
SEUI_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
SEUI_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
SEUI_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
SEUI_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
SEUI_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
SEUI_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?

Table 101. Format of the SETEUID Record Extension (Event Code 50) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
SEUI_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
SEUI_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
SEUI_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
SEUI_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
SEUI_UTK_SNODE	Char	8	413	420	The submitting node.
SEUI_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
SEUI_UTK_SPOE	Char	8	431	438	The port of entry.
SEUI_UTK_SPCCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
SEUI_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
SEUI_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
SEUI_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
SEUI_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
SEUI_APPC_LINK	Char	16	477	492	Key to link together APPC records.
SEUI_AUDIT_CODE	Char	11	494	504	Audit function code.
SEUI_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
SEUI_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
SEUI_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
SEUI_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
SEUI_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
SEUI_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
SEUI_NEW_REAL_UID	Integer	10	572	581	New real z/OS UNIX user identifier (UID).
SEUI_NEW_EFF_UID	Integer	10	583	592	New effective z/OS UNIX user identifier (UID).
SEUI_NEW_SAVED_UID	Integer	10	594	603	New saved z/OS UNIX user identifier (UID).
SEUI_UID	Integer	10	605	614	The z/OS UNIX user identifier (UID) input parameter.
SEUI_DFLT_PROCESS	Yes/No	4	616	619	Default z/OS UNIX security environment in effect.
SEUI_UTK_NETW	Char	8	621	628	The port of entry network name.
SEUI_X500_SUBJECT	Char	255	630	884	Subject's name associated with this event.
SEUI_X500_ISSUER	Char	255	886	1140	Issuer's name associated with this event.

Event Qualifiers for the SETEUID Record Extension

The event qualifiers that may be associated with setting the effective z/OS UNIX user identifier (UID) are shown in Table 102.

Table 102. Event Qualifiers for SETEUID Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Successful change of z/OS UNIX user identifiers (UIDs).
NOTAUTH	01	Not authorized to set the effective z/OS UNIX user identifier (UID).

The Format of the SETGID Record Extension

Table 103 on page 200 describes the format of a record that is created by the setting of a z/OS UNIX group identifier (GID).

SMF Data Unload—IRRADU00

Table 103. Format of the SETGID Record Extension (Event Code 51)

Field Name	Type	Length	Position		Comments
			Start	End	
SGI_CLASS	Char	8	282	289	Class name.
SGI_USER_NAME	Char	20	291	310	The name associated with the user ID.
SGI_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
SGI_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
SGI_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
SGI_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
SGI_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
SGI_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
SGI_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
SGI_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
SGI_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
SGI_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
SGI_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
SGI_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
SGI_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
SGI_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
SGI_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
SGI_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
SGI_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
SGI_UTK_SNODE	Char	8	413	420	The submitting node.
SGI_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
SGI_UTK_SPOE	Char	8	431	438	The port of entry.
SGI_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
SGI_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
SGI_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
SGI_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
SGI_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
SGI_APPC_LINK	Char	16	477	492	Key to link together APPC records.
SGI_AUDIT_CODE	Char	11	494	504	Audit function code.
SGI_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
SGI_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
SGI_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
SGI_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
SGI_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
SGI_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
SGI_NEW_REAL_GID	Integer	10	572	581	New real z/OS UNIX group identifier (GID).
SGI_NEW_EFF_GID	Integer	10	583	592	New effective z/OS UNIX group identifier (GID).
SGI_NEW_SAVED_GID	Integer	10	594	603	New saved z/OS UNIX group identifier (GID).
SGI_GID	Integer	10	605	614	The z/OS UNIX group identifier (GID) input parameter.
SGI_DFLT_PROCESS	Yes/No	4	616	619	Default z/OS UNIX security environment in effect.
SGI_UTK_NETW	Char	8	621	628	The port of entry network name.

Table 103. Format of the SETGID Record Extension (Event Code 51) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
SGL_X500_SUBJECT	Char	255	630	884	Subject's name associated with this event.
SGL_X500_ISSUER	Char	255	886	1140	Issuer's name associated with this event.

Event Qualifiers for the SETGID Record Extension

The event qualifiers that may be associated with setting the z/OS UNIX group identifier (GID) are shown in Table 104.

Table 104. Event Qualifiers for SETGID Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Successful change of z/OS UNIX group identifier (GID).
NOTAUTH	01	Not authorized to set the z/OS UNIX group identifier (GID).

The Format of the SETUID Record Extension

Table 105 describes the format of a record that is created by the setting of a z/OS UNIX user identifier (UID).

Table 105. Format of the SETUID Record Extension (Event Code 52)

Field Name	Type	Length	Position		Comments
			Start	End	
SUI_CLASS	Char	8	282	289	Class name.
SUI_USER_NAME	Char	20	291	310	The name associated with the user ID.
SUI_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
SUI_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
SUI_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
SUI_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
SUI_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
SUI_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
SUI_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
SUI_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
SUI_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
SUI_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
SUI_UTK_SESTYPE	Char	8	362	369	The session type of this session.
SUI_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
SUI_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
SUI_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
SUI_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
SUI_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
SUI_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
SUI_UTK_SNODE	Char	8	413	420	The submitting node.
SUI_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
SUI_UTK_SPOE	Char	8	431	438	The port of entry.

SMF Data Unload—IRRADU00

Table 105. Format of the SETUID Record Extension (Event Code 52) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
SUI_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
SUI_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
SUI_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
SUI_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
SUI_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
SUI_APPC_LINK	Char	16	477	492	Key to link together APPC records.
SUI_AUDIT_CODE	Char	11	494	504	Audit function code.
SUI_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
SUI_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
SUI_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
SUI_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
SUI_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
SUI_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
SUI_NEW_REAL_UID	Integer	10	572	581	New real z/OS UNIX user identifier (UID).
SUI_NEW_EFF_UID	Integer	10	583	592	New effective z/OS UNIX user identifier (UID).
SUI_NEW_SAVED_UID	Integer	10	594	603	New saved z/OS UNIX user identifier (UID).
SUI_UID	Integer	10	605	614	The z/OS UNIX user identifier (UID) input parameter.
SUI_DFLT_PROCESS	Yes/No	4	616	619	Default z/OS UNIX security environment in effect.
SUI_UTK_NETW	Char	8	621	628	The port of entry network name.
SUI_X500_SUBJECT	Char	255	630	884	Subject's name associated with this event.
SUI_X500_ISSUER	Char	255	886	1140	Issuer's name associated with this event.

Event Qualifiers for the SETUID Record Extension

The event qualifiers that may be associated with setting the effective z/OS UNIX user identifier (UID) are shown in Table 106.

Table 106. Event Qualifiers for SETUID Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Successful change of z/OS UNIX user identifier (UID).
NOTAUTH	01	Not authorized to set the z/OS UNIX user identifier (UID).

The Format of the SYMLINK Record Extension

Table 107 describes the format of a record that is created by a SYMLINK operation.

Table 107. Format of the SYMLINK Record Extension (Event Code 53)

Field Name	Type	Length	Position		Comments
			Start	End	
SYML_CLASS	Char	8	282	289	Class name.
SYML_USER_NAME	Char	20	291	310	The name associated with the user ID.
SYML_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?

Table 107. Format of the SYMLINK Record Extension (Event Code 53) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
SYML_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
SYML_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
SYML_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
SYML_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
SYML_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
SYML_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
SYML_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
SYML_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
SYML_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
SYML_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
SYML_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
SYML_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
SYML_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
SYML_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
SYML_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
SYML_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
SYML_UTK_SNODE	Char	8	413	420	The submitting node.
SYML_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
SYML_UTK_SPOE	Char	8	431	438	The port of entry.
SYML_UTK_SPCCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
SYML_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
SYML_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
SYML_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
SYML_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
SYML_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
SYML_AUDIT_CODE	Char	11	494	504	Audit function code.
SYML_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
SYML_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
SYML_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
SYML_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
SYML_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
SYML_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
SYML_PATH_NAME	Char	1023	572	1594	The requested path name.
SYML_FILE_ID	Char	32	1596	1627	File ID.
SYML_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
SYML_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
SYML_SYMLINK_DATA	Char	1023	1651	2673	Content of SYMLINK.
SYML_FILEPOOL	Char	8	2675	2682	SFS filepool containing the BFS file.
SYML_FILESSPACE	Char	8	2684	2691	SFS filespace containing the BFS file.
SYML_INODE	Integer	10	2693	2702	Inode (file serial number).

SMF Data Unload—IRRADU00

Table 107. Format of the SYMLINK Record Extension (Event Code 53) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
SYML_SCID	Integer	10	2704	2713	File SCID.
SYML_DFLT_PROCESS	Char	1	2715	2715	Default z/OS UNIX security environment in effect.
SYML_UTK_NETW	Char	8	2720	2727	The port of entry network name.
SYML_X500_SUBJECT	Char	255	2729	2983	Subject's name associated with this event.
SYML_X500_ISSUER	Char	255	2985	3239	Issuer's name associated with this event.

Event Qualifiers for SYMLINK Records

The event qualifier that may be associated with a SYMLINK event is shown in Table 108.

Table 108. Event Qualifiers for SYMLINK Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Successful SYMLINK. There are no failure cases for this event.

The Format of the UNLINK Record Extension

Table 109 describes the format of a record that is created by an UNLINK operation.

Table 109. Format of the UNLINK Record Extension (Event Code 54)

Field Name	Type	Length	Position		Comments
			Start	End	
UNL_CLASS	Char	8	282	289	Class name.
UNL_USER_NAME	Char	20	291	310	The name associated with the user ID.
UNL_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
UNL_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
UNL_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
UNL_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
UNL_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
UNL_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
UNL_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
UNL_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
UNL_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
UNL_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
UNL_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
UNL_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
UNL_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
UNL_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
UNL_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
UNL_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
UNL_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
UNL_UTK_SNODE	Char	8	413	420	The submitting node.

Table 109. Format of the UNLINK Record Extension (Event Code 54) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
UNL_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
UNL_UTK_SPOE	Char	8	431	438	The port of entry.
UNL_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
UNL_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
UNL_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
UNL_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
UNL_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
UNL_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
UNL_AUDIT_CODE	Char	11	494	504	Audit function code.
UNL_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
UNL_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
UNL_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
UNL_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
UNL_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
UNL_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
UNL_PATH_NAME	Char	1023	572	1594	The requested path name.
UNL_FILE_ID	Char	32	1596	1627	File ID.
UNL_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
UNL_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
UNL_LAST_DELETED	Yes/No	4	1651	1654	Was the last link deleted?
UNL_FILEPOOL	Char	8	1656	1663	SFS filepool containing the BFS file.
UNL_FILESPACE	Char	8	1665	1672	SFS filespace containing the BFS file.
UNL_INODE	Integer	10	1674	1683	Inode (file serial number).
UNL_SCID	Integer	10	1685	1694	File SCID.
UNL_DCE_LINK	Char	16	1696	1711	Link to connect DCE records that originate from a single DCE request.
UNL_AUTH_TYPE	Char	13	1713	1725	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
UNL_DFLT_PROCESS	Yes/No	4	1727	1730	Default z/OS UNIX security environment in effect.
UNL_UTK_NETW	Char	8	1732	1739	The port of entry network name.
UNL_X500_SUBJECT	Char	255	1741	1995	Subject's name associated with this event.
UNL_X500_ISSUER	Char	255	1997	2251	Issuer's name associated with this event.

Event Qualifiers for UNLINK Records

The event qualifier that may be associated with an UNLINK event is shown in Table 110 on page 206.

SMF Data Unload—IRRADU00

Table 110. Event Qualifiers for UNLINK Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Successful UNLINK. Failures are logged as check access event types.

The Format of the Unmount File System Record Extension

Table 111 describes the format of a record that is created unmounting a file system.

Table 111. Format of the Unmount File System Record Extension (Event Code 55)

Field Name	Type	Length	Position		Comments
			Start	End	
UFS_CLASS	Char	8	282	289	Class name.
UFS_USER_NAME	Char	20	291	310	The name associated with the user ID.
UFS_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
UFS_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
UFS_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
UFS_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
UFS_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
UFS_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
UFS_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
UFS_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
UFS_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
UFS_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
UFS_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
UFS_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
UFS_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
UFS_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
UFS_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
UFS_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
UFS_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
UFS_UTK_SNODE	Char	8	413	420	The submitting node.
UFS_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
UFS_UTK_SPOE	Char	8	431	438	The port of entry.
UFS_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
UFS_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
UFS_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
UFS_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
UFS_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
UFS_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
UFS_AUDIT_CODE	Char	11	494	504	Audit function code.
UFS_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
UFS_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
UFS_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).

Table 111. Format of the Unmount File System Record Extension (Event Code 55) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
UFS_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
UFS_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
UFS_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
UFS_PATH_NAME	Char	1023	572	1594	The requested path name.
UFS_FILE_ID	Char	32	1596	1627	File ID.
UFS_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
UFS_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
UFS_HFS_DS_NAME	Char	44	1651	1694	HFS data set name for the mounted file system.
UFS_DCE_LINK	Char	16	1696	1711	Link to connect DCE records that originate from a single DCE request.
UFS_AUTH_TYPE	Char	13	1713	1725	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
UFS_DFLT_PROCESS	Yes/No	4	1727	1730	Default z/OS UNIX security environment in effect.
UFS_UTK_NETW	Char	8	1732	1739	The port of entry network name.
UFS_X500_SUBJECT	Char	255	1741	1995	Subject's name associated with this event.
UFS_X500_ISSUER	Char	255	1997	2251	Issuer's name associated with this event.

Event Qualifiers for Unmount File System Records

The event qualifier that may be associated with the unmounting of a file system is shown in Table 112.

Table 112. Event Qualifiers for Unmount File System Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Unmount successful. Failures are logged as CKPRIV events.

The Format of the Check File Owner Record Extension

Table 113 describes the format of a record that is created by checking the owner of a file.

Table 113. Format of the Check File Owner Record Extension (Event Code 56)

Field Name	Type	Length	Position		Comments
			Start	End	
CFOW_CLASS	Char	8	282	289	Class name.
CFOW_USER_NAME	Char	20	291	310	The name associated with the user ID.
CFOW_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
CFOW_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
CFOW_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
CFOW_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
CFOW_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
CFOW_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
CFOW_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?

SMF Data Unload—IRRADU00

Table 113. Format of the Check File Owner Record Extension (Event Code 56) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
CFOW_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
CFOW_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
CFOW_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
CFOW_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
CFOW_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
CFOW_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
CFOW_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
CFOW_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
CFOW_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
CFOW_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
CFOW_UTK_SNODE	Char	8	413	420	The submitting node.
CFOW_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
CFOW_UTK_SPOE	Char	8	431	438	The port of entry.
CFOW_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
CFOW_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
CFOW_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
CFOW_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
CFOW_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
CFOW_APPC_LINK	Char	16	477	492	Key to link together APPC records.
CFOW_AUDIT_CODE	Char	11	494	504	Audit function code.
CFOW_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
CFOW_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
CFOW_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
CFOW_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
CFOW_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
CFOW_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
CFOW_PATH_NAME	Char	1023	572	1594	The requested path name.
CFOW_FILE_ID	Char	32	1596	1627	File ID.
CFOW_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
CFOW_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
CFOW_FILEPOOL	Char	8	1651	1658	SFS filepool containing the BFS file.
CFOW_FILESPACE	Char	8	1660	1667	SFS filespace containing the BFS file.
CFOW_INODE	Integer	10	1669	1678	Inode (file serial number).
CFOW_SCID	Integer	10	1680	1689	File SCID.
CFOW_DCE_LINK	Char	16	1691	1706	Link to connect DCE records that originate from a single DCE request.
CFOW_AUTH_TYPE	Char	13	1708	1720	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
CFOW_DFLT_PROCESS	Yes/No	4	1722	1725	Default z/OS UNIX security environment in effect.
CFOW_UTK_NETW	Char	8	1727	1734	The port of entry network name.
CFOW_X500_SUBJECT	Char	255	1736	1990	Subject's name associated with this event.

Table 113. Format of the Check File Owner Record Extension (Event Code 56) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
CFLOW_X500_ISSUER	Char	255	1992	2246	Issuer's name associated with this event.

Event Qualifiers for Check File Owner Records

The event qualifiers that may be associated with checking a file's owner are shown in Table 114.

Table 114. Event Qualifiers for Check File Owner Records

Event Qualifier	Event Qualifier Number	Event Description
OWNER	00	The user is the owner.
NOTOWNER	01	The user is not the owner.

The Format of the Check Privilege Record Extension

Table 115 describes the format of a record that is created by checking a user's privileges.

Table 115. Format of the Check Privileges Record Extension (Event Code 57)

Field Name	Type	Length	Position		Comments
			Start	End	
CPRV_CLASS	Char	8	282	289	Class name.
CPRV_USER_NAME	Char	20	291	310	The name associated with the user ID.
CPRV_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
CPRV_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
CPRV_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
CPRV_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
CPRV_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
CPRV_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
CPRV_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
CPRV_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
CPRV_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
CPRV_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
CPRV_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
CPRV_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
CPRV_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
CPRV_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
CPRV_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
CPRV_UTK_EXECPNODE	Char	8	395	402	The execution node of the work.
CPRV_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
CPRV_UTK_SNODE	Char	8	413	420	The submitting node.
CPRV_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
CPRV_UTK_SPOE	Char	8	431	438	The port of entry.
CPRV_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".

SMF Data Unload—IRRADU00

Table 115. Format of the Check Privileges Record Extension (Event Code 57) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
CPRV_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
CPRV_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
CPRV_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
CPRV_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
CPRV_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
CPRV_AUDIT_CODE	Char	11	494	504	Audit function code.
CPRV_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
CPRV_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
CPRV_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
CPRV_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
CPRV_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
CPRV_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
CPRV_DCE_LINK	Char	16	572	587	Link to connect DCE records that originate from a single DCE request.
CPRV_AUTH_TYPE	Char	13	589	601	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
CPRV_DFLT_PROCESS	Yes/No	4	603	606	Default z/OS UNIX security environment in effect.
CPRV_UTK_NETW	Char	8	608	615	The port of entry network name.
CPRV_X500_SUBJECT	Char	255	617	871	Subject's name associated with this event.
CPRV_X500_ISSUER	Char	255	873	1127	Issuer's name associated with this event.

Event Qualifiers for Check Privilege Records

The event qualifiers that may be associated with checking a user's privileges are shown in Table 116.

Table 116. Event Qualifiers for Check Privileges Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	User is authorized.
NOTAUTH	01	The user is not authorized to the function.

The Format of the Open Slave TTY Record Extension

Table 117 describes the format of a record that is created by the opening of a slave TTY.

Table 117. Format of the Open Slave TTY Record Extension (Event Code 58)

Field Name	Type	Length	Position		Comments
			Start	End	
OSTY_CLASS	Char	8	282	289	Class name.
OSTY_USER_NAME	Char	20	291	310	The name associated with the user ID.
OSTY_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
OSTY_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
OSTY_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?

Table 117. Format of the Open Slave TTY Record Extension (Event Code 58) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
OSTY_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
OSTY_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
OSTY_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
OSTY_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
OSTY_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
OSTY_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
OSTY_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
OSTY_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
OSTY_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
OSTY_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
OSTY_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
OSTY_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
OSTY_UTK_EXECPNODE	Char	8	395	402	The execution node of the work.
OSTY_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
OSTY_UTK_SNODE	Char	8	413	420	The submitting node.
OSTY_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
OSTY_UTK_SPOE	Char	8	431	438	The port of entry.
OSTY_UTK_SPCCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
OSTY_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
OSTY_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
OSTY_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
OSTY_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
OSTY_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
OSTY_AUDIT_CODE	Char	11	494	504	Audit function code.
OSTY_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
OSTY_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
OSTY_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
OSTY_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
OSTY_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
OSTY_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
OSTY_TGT_REAL_UID	Integer	10	572	581	Target real z/OS UNIX user identifier (UID).
OSTY_TGT_EFF_UID	Integer	10	583	592	Target effective z/OS UNIX user identifier (UID).
OSTY_TGT_SAV_UID	Integer	10	594	603	Target saved z/OS UNIX user identifier (UID).
OSTY_TGT_PID	Integer	10	605	614	Target process ID.
OSTY_DFLT_PROCESS	Yes/No	4	616	619	Default z/OS UNIX security environment in effect.
OSTY_UTK_NETW	Char	8	621	628	The port of entry network name.
OSTY_X500_SUBJECT	Char	255	630	884	Subject's name associated with this event.
OSTY_X500_ISSUER	Char	255	886	1140	Issuer's name associated with this event.

Event Qualifiers for Open Slave TTY Records

The event qualifiers that may be associated with open slave TTY records are shown in Table 118 on page 212.

SMF Data Unload—IRRADU00

Table 118. Event Qualifiers for Open Slave TTY Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Access allowed.
NOTAUTH	01	Not authorized to the specified process.

The Format of the RACLINK Command Record Extension

Table 119 describes the format of a record that is created by the a RACLINK command.

Table 119. Format of the RACLINK Command Record Extension (Event Code 59)

Field Name	Type	Length	Position		Comments
			Start	End	
RACL_USER_NAME	Char	20	282	301	The name associated with the user ID.
RACL_UTK_ENCR	Yes/No	4	303	306	Is the UTOKEN associated with this user encrypted?
RACL_UTK_PRE19	Yes/No	4	308	311	Is this a pre-1.9 token?
RACL_UTK_VERPROF	Yes/No	4	313	316	Is the VERIFYX propagation flag set?
RACL_UTK_NJEUNUSR	Yes/No	4	318	321	Is this the NJE undefined user?
RACL_UTK_LOGUSR	Yes/No	4	323	326	Is UAUDIT specified for this user?
RACL_UTK_SPECIAL	Yes/No	4	328	331	Is this a SPECIAL user?
RACL_UTK_DEFAULT	Yes/No	4	333	336	Is this a default token?
RACL_UTK_UNKNUSR	Yes/No	4	338	341	Is this an undefined user?
RACL_UTK_ERROR	Yes/No	4	343	346	Is this user token in error?
RACL_UTK_TRUSTED	Yes/No	4	348	351	Is this user a part of the trusted computing base (TCB)?
RACL_UTK_SESSTYPE	Char	8	353	360	The session type of this session.
RACL_UTK_SURROGAT	Yes/No	4	362	365	Is this a surrogate user?
RACL_UTK_REMOTE	Yes/No	4	367	370	Is this a remote job?
RACL_UTK_PRIV	Yes/No	4	372	375	Is this a privileged user ID?
RACL_UTK_SECL	Char	8	377	384	The SECLABEL of the user.
RACL_UTK_EXECPNODE	Char	8	386	393	The execution node of the work.
RACL_UTK_SUSER_ID	Char	8	395	402	The submitting user ID.
RACL_UTK_SNODE	Char	8	404	411	The submitting node.
RACL_UTK_SGRP_ID	Char	8	413	420	The submitting group name.
RACL_UTK_SPOE	Char	8	422	429	The port of entry.
RACL_UTK_SPCCLASS	Char	8	431	438	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
RACL_UTK_USER_ID	Char	8	440	447	User ID associated with the record.
RACL_UTK_GRP_ID	Char	8	449	456	Group name associated with the record.
RACL_UTK_DFT_GRP	Yes/No	4	458	461	Is a default group assigned?
RACL_UTK_DFT_SECL	Yes/No	4	463	466	Is a default SECLABEL assigned?
RACL_PHASE	Char	20	468	487	Phase of this RACF command. Valid values are "LOCAL ISSUANCE", "TARGET PROCESSING", and "TARGET RESPONSE".
RACL_ISSUE_NODE	Char	8	489	496	Node that originated the command.
RACL_ISSUE_ID	Char	8	498	505	User ID that originated the command.
RACL_SOURCE_ID	Char	8	507	514	User ID for the association. From the ID keyword.

Table 119. Format of the RACLINK Command Record Extension (Event Code 59) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
RACL_TGT_NODE	Char	8	516	523	Node that is the destination of the command.
RACL_TGT_ID	Char	8	525	532	User ID that is the destination of the command.
RACL_TGT_AUTH_ID	Char	8	534	541	User ID under whose authority the association is established.
RACL_SOURCE_SMFID	Char	4	543	546	SMF system identifier of the system that originated the command.
RACL_SOURCE_TIME	Char	8	548	555	Time that the command originated.
RACL_SOURCE_DATE	Char	10	557	566	Date that the command originated.
RACL_PWD_STATUS	Char	8	568	575	Status of the password sent with the command. Valid values are: SUPPLIED A password was supplied on a DEFINE command. This value occurs only for a LOCAL ISSUANCE phase record or for a TARGET PROCESSING phase when the event number is 3. VALID The password that was supplied on a DEFINE command is correct. This value occurs only for TARGET PROCESSING and TARGET RESPONSE phase records. NOTVALID The password that was supplied on a DEFINE command is not correct. This value occurs only for a TARGET PROCESSING phase record. EXPIRED The password that was supplied on a DEFINE command is expired. This value occurs for a TARGET PROCESSING only. REVOKED The target user ID on the DEFINE command is revoked. This value occurs for a TARGET PROCESSING phase only. NONE No password was supplied for the DEFINE command. This value can occur for any phase record. A blank value indicates that an UNDEFINE or APPROVE command was issued. Neither of these commands have passwords.
RACL_ASSOC_STATUS	Char	8	577	584	Status of the association. Valid values are "PENDING", "ESTAB", and "DELETED".
RACL_SPECIFIED	Char	1024	586	1609	The keywords specified.
RACL_UTK_NETW	Char	8	1611	1618	The port of entry network name.
RACL_X500_SUBJECT	Char	255	1620	1874	Subject's name associated with this event.
RACL_X500_ISSUER	Char	255	1876	2130	Issuer's name associated with this event.

Note: Records created for user IDs which are revoked have no UTKEN information.

Event Qualifiers for the RACLINK Command Records

The event qualifiers that may be associated with the RACLINK command are shown in Table 120.

Table 120. Event Qualifiers for RACLINK Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Command successful.
INSAUTH	01	Insufficient authority (local issuance only).
-----	02	Reserved.
ALRDYDEF	03	Association already defined.
ALRDYAPP	04	Association already approved.
NOMATCH	05	Association does not match.
NOTEXIST	06	Association does not exist.
INVPSWD	07	Invalid password.

The Format of the IPCCHK Record Extension

Table 121 describes the format of a record that is created by checking access to an IPC.

Table 121. Format of the IPCCHK Record Extension (Event Code 60)

Field Name	Type	Length	Position		Comments
			Start	End	
ICLK_CLASS	Char	8	282	289	Class name.
ICLK_USER_NAME	Char	20	291	310	The name associated with the user ID.
ICLK_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
ICLK_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
ICLK_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
ICLK_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
ICLK_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
ICLK_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
ICLK_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
ICLK_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
ICLK_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
ICLK_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
ICLK_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
ICLK_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
ICLK_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
ICLK_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
ICLK_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
ICLK_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
ICLK_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
ICLK_UTK_SNODE	Char	8	413	420	The submitting node.
ICLK_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
ICLK_UTK_SPOE	Char	8	431	438	The port of entry.

Table 121. Format of the IPCCHK Record Extension (Event Code 60) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
ICLK_UTK_SPCCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
ICLK_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
ICLK_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
ICLK_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
ICLK_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
ICLK_APPC_LINK	Char	16	477	492	Key to link together APPC records.
ICLK_AUDIT_CODE	Char	11	494	504	Audit function code. For more information on the function codes, see <i>z/OS Security Server RACF Callable Services</i> .
ICLK_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
ICLK_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
ICLK_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
ICLK_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
ICLK_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
ICLK_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
ICLK_KEY_OWN_UID	Integer	10	572	581	The owner z/OS UNIX user identifier (UID) associated with the key.
ICLK_KEY_OWN_GID	Integer	10	583	592	The owner z/OS UNIX group identifier (GID) associated with the key.
ICLK_REQUEST_READ	Yes/No	4	594	597	Did the requested access include read?
ICLK_REQUEST_WRITE	Yes/No	4	599	602	Did the requested access include write?
ICLK_REQUEST_EXEC	Yes/No	4	604	607	Did the requested access include execute?
ICLK_RESERVED_01	Yes/No	4	609	612	Reserved.
ICLK_ACCESS_TYPE	Char	8	614	621	What bits were used in granting the access? Valid values are "OWNER", "GROUP", "NO", and "OTHER".
ICLK_ALLOWED_READ	Yes/No	4	623	626	Was read access allowed?
ICLK_ALLOWED_WRITE	Yes/No	4	628	631	Was write access allowed?
ICLK_RESERVED_02	Yes/No	4	633	636	Reserved.
ICLK_KEY	Char	8	638	645	The key of the IPC resource.
ICLK_ID	Integer	10	647	656	The unique decimal identifier of the IPC resource.
ICLK_CREATOR_UID	Integer	10	658	667	The z/OS UNIX user identifier (UID) of the creator.
ICLK_CREATOR_GID	Integer	10	669	678	The z/OS UNIX group identifier (GID) of the creator.
ICLK_DFLT_PROCESS	Yes/No	4	680	683	Default z/OS UNIX security environment in effect.
ICLK_UTK_NETW	Char	8	685	692	The port of entry network name.
ICLK_X500_SUBJECT	Char	255	694	948	Subject's name associated with this event.
ICLK_X500_ISSUER	Char	255	950	1204	Issuer's name associated with this event.

Event Qualifiers for IPCCHK Records

The event qualifiers that may be associated with a check IPC event are shown in Table 122 on page 216.

SMF Data Unload—IRRADU00

Table 122. Event Qualifiers for Check IPC Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Access allowed.
NOTAUTH	01	Not authorized to the resource.

The Format of the IPCGET Record Extension

Table 123 describes the format of a record that is created by creating an IPC.

Table 123. Format of the IPCGET Record Extension (Event Code 61)

Field Name	Type	Length	Position		Comments
			Start	End	
IGET_CLASS	Char	8	282	289	Class name.
IGET_USER_NAME	Char	20	291	310	The name associated with the user ID.
IGET_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
IGET_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
IGET_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
IGET_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
IGET_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
IGET_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
IGET_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
IGET_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
IGET_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
IGET_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
IGET_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
IGET_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
IGET_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
IGET_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
IGET_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
IGET_UTK_EXECCODE	Char	8	395	402	The execution node of the work.
IGET_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
IGET_UTK_SNODE	Char	8	413	420	The submitting node.
IGET_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
IGET_UTK_SPOE	Char	8	431	438	The port of entry.
IGET_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
IGET_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
IGET_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
IGET_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
IGET_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
IGET_APPC_LINK	Char	16	477	492	Key to link together APPC records.
IGET_AUDIT_CODE	Char	11	494	504	Audit function code. For more information on the function codes, see <i>z/OS Security Server RACF Callable Services</i> .
IGET_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).

Table 123. Format of the IPCGET Record Extension (Event Code 61) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
IGET_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
IGET_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
IGET_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
IGET_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
IGET_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
IGET_KEY_OWN_UID	Integer	10	572	581	The owner z/OS UNIX user identifier (UID) associated with the key.
IGET_KEY_OWN_GID	Integer	10	583	592	The owner z/OS UNIX group identifier (GID) associated with the key.
IGET_RESERVED_01	Yes/No	4	594	597	Reserved.
IGET_RESERVED_02	Yes/No	4	599	602	Reserved.
IGET_RESERVED_03	Yes/No	4	604	607	Reserved.
IGET_REQ_OWN_READ	Yes/No	4	609	612	Was the owner READ bit requested on for this file?
IGET_REQ_OWN_WRITE	Yes/No	4	614	617	Was the owner WRITE bit requested on for this file?
IGET_REQ_OWN_EXEC	Yes/No	4	619	622	Was the owner EXECUTE bit requested on for this file?
IGET_REQ_GRP_READ	Yes/No	4	624	627	Was the group READ bit requested on for this file?
IGET_REQ_GRP_WRITE	Yes/No	4	629	632	Was the group WRITE bit requested on for this file?
IGET_REQ_GRP_EXEC	Yes/No	4	634	637	Was the group EXECUTE bit requested on for this file?
IGET_REQ_OTH_READ	Yes/No	4	639	642	Was the other READ bit requested on for this file?
IGET_REQ_OTH_WRITE	Yes/No	4	644	647	Was the other WRITE bit requested on for this file?
IGET_REQ_OTH_EXEC	Yes/No	4	649	652	Was the other EXECUTE bit requested on for this file?
IGET_KEY	Char	8	654	661	The key of the IPC resource.
IGET_ID	Integer	10	663	672	The unique decimal identifier of the IPC resource.
IGET_CREATOR_UID	Integer	10	674	683	The z/OS UNIX user identifier (UID) of the creator.
IGET_CREATOR_GID	Integer	10	685	694	The z/OS UNIX group identifier (GID) of the creator.
IGET_DFLT_PROCESS	Yes/No	4	696	699	Default z/OS UNIX security environment in effect.
IGET_UTK_NETW	Char	8	701	708	The port of entry network name.
IGET_X500_SUBJECT	Char	255	710	964	Subject's name associated with this event.
IGET_X500_ISSUER	Char	255	966	1220	Issuer's name associated with this event.

Event Qualifiers for IPCGET Records

The event qualifiers that may be associated with an IPCGET event are shown in Table 124 on page 218.

SMF Data Unload—IRRADU00

Table 124. Event Qualifiers for IPCGET Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Access allowed.

The Format of the IPCCTL Record Extension

Table 125 describes the format of a record that is created by the IPCCTL function.

Table 125. Format of the IPCCTL Record Extension (Event Code 62)

Field Name	Type	Length	Position		Comments
			Start	End	
ICTL_CLASS	Char	8	282	289	Class name.
ICTL_USER_NAME	Char	20	291	310	The name associated with the user ID.
ICTL_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
ICTL_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
ICTL_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
ICTL_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
ICTL_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
ICTL_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
ICTL_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
ICTL_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
ICTL_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
ICTL_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
ICTL_UTK_SESTYPE	Char	8	362	369	The session type of this session.
ICTL_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
ICTL_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
ICTL_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
ICTL_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
ICTL_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
ICTL_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
ICTL_UTK_SNODE	Char	8	413	420	The submitting node.
ICTL_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
ICTL_UTK_SPOE	Char	8	431	438	The port of entry.
ICTL_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
ICTL_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
ICTL_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
ICTL_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
ICTL_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
ICTL_APPC_LINK	Char	16	477	492	Key to link together APPC records.
ICTL_AUDIT_CODE	Char	11	494	504	Audit function code. For more information on the function codes, see <i>z/OS Security Server RACF Callable Services</i> .
ICTL_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
ICTL_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).

Table 125. Format of the IPCCTL Record Extension (Event Code 62) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
ICTL_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
ICTL_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
ICTL_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
ICTL_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
ICTL_KEY_OWN_UID	Integer	10	572	581	The owner z/OS UNIX user identifier (UID) associated with the key
ICTL_KEY_OWN_GID	Integer	10	583	592	The owner z/OS UNIX group identifier (GID) associated with the key.
ICTL_UID	Integer	10	594	603	The owner z/OS UNIX user identifier (UID) input parameter.
ICTL_GID	Integer	10	605	614	The owner z/OS UNIX group identifier (GID) input parameter.
ICTL_RESERVED_01	Yes/No	4	616	619	Reserved.
ICTL_RESERVED_02	Yes/No	4	621	624	Reserved.
ICTL_RESERVED_03	Yes/No	4	626	629	Reserved.
ICTL_OLD_OWN_READ	Yes/No	4	631	634	Was the owner READ bit on for this file?
ICTL_OLD_OWN_WRITE	Yes/No	4	636	639	Was the owner WRITE bit on for this file?
ICTL_OLD_OWN_EXEC	Yes/No	4	641	644	Was the owner EXECUTE bit on for this file?
ICTL_OLD_GRP_READ	Yes/No	4	646	649	Was the group READ bit on for this file?
ICTL_OLD_GRP_WRITE	Yes/No	4	651	654	Was the group WRITE bit on for this file?
ICTL_OLD_GRP_EXEC	Yes/No	4	656	659	Was the group EXECUTE bit on for this file?
ICTL_OLD_OTH_READ	Yes/No	4	661	664	Was the other READ bit on for this file?
ICTL_OLD_OTH_WRITE	Yes/No	4	666	669	Was the other WRITE bit on for this file?
ICTL_OLD_OTH_EXEC	Yes/No	4	671	674	Was the other EXECUTE bit on for this file?
ICTL_RESERVED_04	Yes/No	4	676	679	Reserved.
ICTL_RESERVED_05	Yes/No	4	681	684	Reserved.
ICTL_RESERVED_06	Yes/No	4	686	689	Reserved.
ICTL_NEW_OWN_READ	Yes/No	4	691	694	Is the owner READ bit on for this file?
ICTL_NEW_OWN_WRITE	Yes/No	4	696	699	Is the owner WRITE bit on for this file?
ICTL_NEW_OWN_EXEC	Yes/No	4	701	704	Is the owner EXECUTE bit on for this file?
ICTL_NEW_GRP_READ	Yes/No	4	706	709	Is the group READ bit on for this file?
ICTL_NEW_GRP_WRITE	Yes/No	4	711	714	Is the group WRITE bit on for this file?
ICTL_NEW_GRP_EXEC	Yes/No	4	716	719	Is the group EXECUTE bit on for this file?
ICTL_NEW_OTH_READ	Yes/No	4	721	724	Is the other READ bit on for this file?
ICTL_NEW_OTH_WRITE	Yes/No	4	726	729	Is the other WRITE bit on for this file?
ICTL_NEW_OTH_EXEC	Yes/No	4	731	734	Is the other EXECUTE bit on for this file?
ICTL_SERVICE_CODE	Char	11	736	746	The service that was being processed.
ICTL_RESERVED_07	Yes/No	4	748	751	Reserved.
ICTL_RESERVED_08	Yes/No	4	753	756	Reserved.
ICTL_RESERVED_09	Yes/No	4	758	761	Reserved.
ICTL_REQ_OWN_READ	Yes/No	4	763	766	Was the owner READ bit requested on for this file?
ICTL_REQ_OWN_WRITE	Yes/No	4	768	771	Was the owner WRITE bit requested on for this file?
ICTL_REQ_OWN_EXEC	Yes/No	4	773	776	Was the owner EXECUTE bit requested on for this file?

SMF Data Unload—IRRADU00

Table 125. Format of the IPCCTL Record Extension (Event Code 62) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
ICTL_REQ_GRP_READ	Yes/No	4	778	781	Was the group READ bit requested on for this file?
ICTL_REQ_GRP_WRITE	Yes/No	4	783	786	Was the group WRITE bit requested on for this file?
ICTL_REQ_GRP_EXEC	Yes/No	4	788	791	Was the group EXECUTE bit requested on for this file?
ICTL_REQ_OTH_READ	Yes/No	4	793	796	Was the other READ bit requested on for this file?
ICTL_REQ_OTH_WRITE	Yes/No	4	798	801	Was the other WRITE bit requested on for this file?
ICTL_REQ_OTH_EXEC	Yes/No	4	803	806	Was the other EXECUTE bit requested on for this file?
ICTL_KEY	Char	8	808	815	The key of the IPC resource.
ICTL_ID	Integer	10	817	826	The unique decimal identifier of the IPC resource.
ICTL_CREATOR_UID	Integer	10	828	837	The z/OS UNIX user identifier (UID) of the creator.
ICTL_CREATOR_GID	Integer	10	839	848	The z/OS UNIX group identifier (GID) of the creator.
ICTL_DFLT_PROCESS	Yes/No	4	850	853	Default z/OS UNIX security environment in effect.
ICTL_UTK_NETW	Char	8	855	862	The port of entry network name.
ICTL_X500_SUBJECT	Char	255	864	1118	Subject's name associated with this event.
ICTL_X500_ISSUER	Char	255	1120	1374	Issuer's name associated with this event.

Event Qualifiers for IPCCTL Records

The event qualifiers that may be associated with a IPCCTL event are shown in Table 126.

Table 126. Event Qualifiers for IPCCTL Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Access allowed.
NOTAUTH	01	Not authorized to the resource.

The Format of the SETGROUP Record Extension

Table 127 describes the format of a record that is created by checking the owner of a file.

Table 127. Format of the SETGROUP Record Extension (Event Code 63)

Field Name	Type	Length	Position		Comments
			Start	End	
SETG_CLASS	Char	8	282	289	Class name.
SETG_USER_NAME	Char	20	291	310	The name associated with the user ID.
SETG_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
SETG_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
SETG_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
SETG_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?

Table 127. Format of the SETGROUP Record Extension (Event Code 63) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
SETG_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
SETG_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
SETG_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
SETG_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
SETG_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
SETG_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
SETG_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
SETG_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
SETG_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
SETG_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
SETG_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
SETG_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
SETG_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
SETG_UTK_SNODE	Char	8	413	420	The submitting node.
SETG_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
SETG_UTK_SPOE	Char	8	431	438	The port of entry.
SETG_UTK_SPCCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
SETG_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
SETG_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
SETG_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
SETG_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
SETG_APPC_LINK	Char	16	477	492	A key to link together audit record together for a user's APPC transaction processing work.
SETG_AUDIT_CODE	Char	11	494	504	Audit function code. For more information on the function codes, see <i>z/OS Security Server RACF Callable Services</i> .
SETG_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
SETG_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
SETG_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
SETG_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
SETG_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
SETG_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
SETG_DCE_LINK	Char	16	572	587	Link to connect DCE records that originate from a single DCE request.
SETG_AUTH_TYPE	Char	13	589	601	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
SETG_DFLT_PROCESS	Yes/No	4	603	606	Default z/OS UNIX security environment in effect.
SETG_UTK_NETW	Char	8	608	615	The port of entry network name.
SETG_X500_SUBJECT	Char	255	617	871	Subject's name associated with this event.
SETG_X500_ISSUER	Char	255	873	1127	Issuer's name associated with this event.

Event Qualifiers for SETGROUP Record Extension

The event qualifiers that may be associated with the SETGROUP function are shown in Table 128.

Table 128. Event Qualifiers for SETGROUP Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Process successfully initialized.
NOTAUTH	01	User does not have the super user authority.

The Format of the CKOWN2 Record Extension

Table 129 describes the format of a record that is created by checking the owner of a file.

Table 129. Format of the CKOWN2 Record Extension (Event Code 64)

Field Name	Type	Length	Position		Comments
			Start	End	
CKO2_CLASS	Char	8	282	289	Class name.
CKO2_USER_NAME	Char	20	291	310	The name associated with the user ID.
CKO2_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
CKO2_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
CKO2_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
CKO2_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
CKO2_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
CKO2_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
CKO2_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
CKO2_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
CKO2_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
CKO2_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
CKO2_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
CKO2_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
CKO2_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
CKO2_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
CKO2_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
CKO2_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
CKO2_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
CKO2_UTK_SNODE	Char	8	413	420	The submitting node.
CKO2_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
CKO2_UTK_SPOE	Char	8	431	438	The port of entry.
CKO2_UTK_SPCCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
CKO2_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
CKO2_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
CKO2_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
CKO2_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
CKO2_APPC_LINK	Char	16	477	492	Key to link together APPC records.

Table 129. Format of the CKOWN2 Record Extension (Event Code 64) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
CKO2_AUDIT_CODE	Char	11	494	504	Audit function code. For more information on the function codes, see <i>z/OS Security Server RACF Callable Services</i> .
CKO2_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
CKO2_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
CKO2_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
CKO2_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
CKO2_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
CKO2_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
CKO2_PATH_NAME	Char	1023	572	1594	The requested path name.
CKO2_FILE1_ID	Char	32	1596	1627	First file ID.
CKO2_FILE1_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the first file.
CKO2_FILE1_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the first file.
CKO2_FILE2_ID	Char	32	1651	1682	Second requested file ID.
CKO2_FILE2_OWN_UID	Integer	10	1684	1693	z/OS UNIX user identifier (UID) of the owner of the second file.
CKO2_FILE2_OWN_GID	Integer	10	1695	1704	z/OS UNIX group identifier (GID) of the owner of the second file.
CKO2_DCE_LINK	Char	16	1706	1721	Link to connect DCE records that originate from a single DCE request.
CKO2_AUTH_TYPE	Char	13	1723	1735	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
CKO2_DFLT_PROCESS	Yes/No	4	1737	1740	Default z/OS UNIX security environment in effect.
CKO2_UTK_NETW	Char	8	1742	1749	The port of entry network name.
CKO2_X500_SUBJECT	Char	255	1751	2005	Subject's name associated with this event.
CKO2_X500_ISSUER	Char	255	2007	2261	Issuer's name associated with this event.

Event Qualifiers for CKOWN2 Records

The event qualifiers that may be associated with checking a file's owner are shown in Table 130.

Table 130. Event Qualifiers for CKOWN2 Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Access allowed.
NOTOWNER	01	The user is not the owner.

The Format of the Access Rights Record Extension

Table 131 on page 224 describes the format of a record that is created when access rights are passed.

SMF Data Unload—IRRADU00

Table 131. Format of the Access Rights Record Extension (Event Code 65)

Field Name	Type	Length	Position		Comments
			Start	End	
ACCR_CLASS	Char	8	282	289	Class name.
ACCR_USER_NAME	Char	20	291	310	The name associated with the user ID
ACCR_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
ACCR_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
ACCR_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
ACCR_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
ACCR_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
ACCR_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
ACCR_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
ACCR_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
ACCR_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
ACCR_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
ACCR_UTK_SESSTYPE	Char	8	362	369	The session type of this session
ACCR_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
ACCR_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
ACCR_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
ACCR_UTK_SECL	Char	8	386	393	The SECLABEL of the user
ACCR_UTK_EXECNODE	Char	8	395	402	The execution node of the work
ACCR_UTK_SUSER_ID	Char	8	404	411	The submitting user ID
ACCR_UTK_SNODE	Char	8	413	420	The submitting node
ACCR_UTK_SGRP_ID	Char	8	422	429	The submitting group name
ACCR_UTK_SPOE	Char	8	431	438	The port of entry
ACCR_UTK_SPCCLASS	Char	8	440	447	Class of the POE Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT"
ACCR_UTK_USER_ID	Char	8	449	456	User ID associated with the record
ACCR_UTK_GRP_ID	Char	8	458	465	Group name associated with the record
ACCR_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
ACCR_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
ACCR_APPC_LINK	Char	16	477	492	Key to link together APPC records
ACCR_AUDIT_CODE	Char	11	494	504	Audit function code
ACCR_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID)
ACCR_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).
ACCR_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
ACCR_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
ACCR_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
ACCR_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
ACCR_PATH_NAME	Char	1023	572	1594	The requested path name
ACCR_FILE1_ID	Char	32	1596	1627	File ID
ACCR_DFLT_PROCESS	Yes/No	4	1629	1632	Default z/OS UNIX security environment in effect.
ACCR_UTK_NETW	Char	8	1634	1641	The port of entry network name.
ACCR_X500_SUBJECT	Char	255	1643	1897	Subject's name associated with this event.
ACCR_X500_ISSUER	Char	255	1899	2153	Issuer's name associated with this event.

Event Qualifiers for Access Rights Records

The event qualifier that may be associated with access rights records are shown in Table 132.

Table 132. Event Qualifiers for Access Rights Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Access rights are passed. There are no failure cases for this event.

The Format of the RACDCERT Command Record Extension

Table 133 describes the format of a record that is created by the RACDCERT command.

Table 133. Format of the RACDCERT Command Extension (Event Code 66)

Field Name	Type	Length	Position		Comments
			Start	End	
RACD_USER_NAME	Char	20	282	301	The name associated with the user ID.
RACD_UTK_ENCR	Yes/No	4	303	306	Is the UTOKEN associated with this user encrypted?
RACD_UTK_PRE19	Yes/No	4	308	311	Is this a pre-1.9 token?
RACD_UTK_VERPROF	Yes/No	4	313	316	Is the VERIFYX propagation flag set?
RACD_UTK_NJEUNUSR	Yes/No	4	318	321	Is this the NJE undefined user?
RACD_UTK_LOGUSR	Yes/No	4	323	326	Is UAUDIT specified for this user?
RACD_UTK_SPECIAL	Yes/No	4	328	331	Is this a SPECIAL user?
RACD_UTK_DEFAULT	Yes/No	4	333	336	Is this a default token?
RACD_UTK_UNKNUSR	Yes/No	4	338	341	Is this an undefined user?
RACD_UTK_ERROR	Yes/No	4	343	346	Is this user token in error?
RACD_UTK_TRUSTED	Yes/No	4	348	351	Is this user a part of the trusted computing base (TCG)?
RACD_UTK_SESSTYPE	Char	8	353	360	The session type of this session.
RACD_UTK_SURROGAT	Yes/No	4	362	365	Is this a surrogate user?
RACD_UTK_REMOTE	Yes/No	4	367	370	Is this a remote job?
RACD_UTK_PRIV	Yes/No	4	372	375	Is this a privileged user ID?
RACD_UTK_SECL	Char	8	377	384	The SECLABEL of the user.
RACD_UTK_EXECNODE	Char	8	386	393	The execution node of the work.
RACD_UTK_SUSER_ID	Char	8	395	402	The submitting user ID.
RACD_UTK_SNODE	Char	8	404	411	The submitting node.
RACD_UTK_SGRP_ID	Char	8	413	420	The submitting group name.
RACD_UTK_SPOE	Char	8	422	429	The port of entry.
RACD_UTK_SPCLASS	Char	8	431	438	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT"
RACD_UTK_USER_ID	Char	8	440	447	User ID associated with the record.
RACD_UTK_GRP_ID	Char	8	449	456	Group name associated with the record.
RACD_UTK_DFT_GRP	Yes/No	4	458	461	Is a default group assigned?
RACD_UTK_DFT_SECL	Yes/No	4	463	466	Is a default SECLABEL assigned?
RACD_SERIAL_NUMBER	Char	255	468	722	Certificate serial number.
RACD_ISSUERS_DN	Char	255	724	978	Certificate issuer's distinguished name.
RACD_CERT_DS	Char	44	980	1023	Data set name containing the certificate.

SMF Data Unload—IRRADU00

Table 133. Format of the RACDCERT Command Extension (Event Code 66) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
RACD_SPECIFIED	Char	1024	1025	2048	The keywords specified.
RACD_UTK_NETW	Char	8	2050	2057	The port of entry network name.
RACD_X500_SUBJECT	Char	255	2059	2313	Subject's name associated with this event.
RACD_X500_ISSUER	Char	255	2315	2569	Issuer's name associated with this event.

Event Qualifiers for the RACDCERT Command Records

The event qualifiers that may be associated with the RACDCERT command are shown in Table 134.

Table 134. Event Qualifiers for RACDCERT Command Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Command successful.
INSAUTH	01	Insufficient authority.

The Format of the InitACEE Record Extension

Table 135 describes the format of a record that is created by InitACEE.

Table 135. Format of the InitACEE Record Extension (Event Code 67)

Field Name	Type	Length	Position		Comments
			Start	End	
INTA_USER_NAME	Char	20	282	301	The name associated with the user ID.
INTA_UTK_ENCR	Yes/No	4	303	306	Is the UTOKEN associated with this user encrypted?
INTA_UTK_PRE19	Yes/No	4	308	311	Is this a pre-1.9 token?
INTA_UTK_VERPROF	Yes/No	4	313	316	Is the VERIFYX propagation flag set?
INTA_UTK_NJEUNUSR	Yes/No	4	318	321	Is this the NJE undefined user?
INTA_UTK_LOGUSR	Yes/No	4	323	326	Is UAUDIT specified for this user?
INTA_UTK_SPECIAL	Yes/No	4	328	331	Is this a SPECIAL user?
INTA_UTK_DEFAULT	Yes/No	4	333	336	Is this a default token?
INTA_UTK_UNKNUSR	Yes/No	4	338	341	Is this an undefined user?
INTA_UTK_ERROR	Yes/No	4	343	346	Is this user token in error?
INTA_UTK_TRUSTED	Yes/No	4	348	351	Is this user a part of the trusted computing base (TCB)?
INTA_UTK_SESTYPE	Char	8	353	360	The session type of this session.
INTA_UTK_SURROGAT	Yes/No	4	362	365	Is this a surrogate user?
INTA_UTK_REMOTE	Yes/No	4	367	370	Is this a remote job?
INTA_UTK_PRIV	Yes/No	4	372	375	Is this a privileged user ID?
INTA_UTK_SECL	Char	8	377	384	The SECLABEL of the user.
INTA_UTK_EXECNODE	Char	8	386	393	The execution node of the work.
INTA_UTK_SUSER_ID	Char	8	395	402	The submitting user ID.
INTA_UTK_SNODE	Char	8	404	411	The submitting node.
INTA_UTK_SGRP_ID	Char	8	413	420	The submitting group name.
INTA_UTK_SPOE	Char	8	422	429	The port of entry.

Table 135. Format of the InitACEE Record Extension (Event Code 67) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
INTA_UTK_SPCLASS	Char	8	431	438	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT"
INTA_UTK_USER_ID	Char	8	440	447	User ID associated with the record.
INTA_UTK_GRP_ID	Char	8	449	456	Group name associated with the record.
INTA_UTK_DFT_GRP	Yes/No	4	458	461	Is a default group assigned?
INTA_UTK_DFT_SECL	Yes/No	4	463	466	Is a default SECLABEL assigned?
INTA_SERIAL_NUMBER	Char	255	468	722	Certificate serial number.
INTA_ISSUERS_DN	Char	255	724	978	Certificate issuer's distinguished name.
INTA_UTK_NETW	Char	8	980	987	The port of entry network name.
INTA_X500_SUBJECT	Char	255	989	1243	Subject's name associated with this event.
INTA_X500_ISSUER	Char	255	1245	1499	Issuer's name associated with this event.

Event Qualifiers for the InitACEE Records

The event qualifiers that may be associated with InitACEE records are shown in Table 136.

Table 136. Event Qualifiers for InitACEE Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCSREG	00	Successful certificate registration.
SUCCSDER	01	Successful certificate deregistration.
INSAUREG	02	Insufficient authority to register the certificate.
INSAUDER	03	Insufficient authority to deregister the certificate.
NOUSRFND	04	No user ID found for the certificate.
CERNTRS	05	The certificate is not trusted.
SUCCSRCA	06	Successful CERTAUTH certificate registration.
INSAURCA	07	Insufficient authority to register the CERTAUTH certificate.

The Format of the Network Authentication Service Record Extension

Table 137 describes the format of a record that is created by the Network Authentication Service.

Table 137. Format of the Network Authentication Service Record Extension (Event Code 68)

Field Name	Type	Length	Position		Comments
			Start	End	
KTKT_PRINCIPAL	Char	240	282	521	The Kerberos principal name.
KTKT_LOGIN_SOURCE	Char	22	523	544	The Kerberos login request source.
KTKT_KDC_STAT_CODE	Char	10	546	555	The Kerberos KDC status code.

Event Qualifiers for the Network Authentication Service Records

The event qualifiers that may be associated with Network Authentication Service records are shown in Table 138 on page 228.

SMF Data Unload—IRRADU00

Table 138. Event Qualifiers for Network Authentication Service Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Successful grant of initial Kerberos ticket.
FAILURE	01	Unsuccessful grant of initial Kerberos ticket.

The Format of the RPKIGENC Record Extension

Table 139 describes the format of a record that is created by RPKIGENC.

Table 139. Format of the RPKIGENC Record Extension (Event Code 69)

Field Name	Type	Length	Position		Comments
			Start	End	
RPKG_LOGSTRING	Char	255	282	536	Logstring parameter.
RPKG_USER_NAME	Char	20	538	557	The name associated with the user ID.
RPKG_UTK_ENCR	Yes/No	4	559	562	Is the UTOKEN associated with this user encrypted?
RPKG_UTK_PRE19	Yes/No	4	564	567	Is this a pre-1.9 token?
RPKG_UTK_VERPROF	Yes/No	4	569	572	Is the VERIFYX propagation?
RPKG_UTK_NJEUNUSR	Yes/No	4	574	577	Is this the NJE undefined user?
RPKG_UTK_LOGUSR	Yes/No	4	579	582	Is UAUDIT specified for this user?
RPKG_UTK_SPECIAL	Yes/No	4	584	587	Is this a SPECIAL user?
RPKG_UTK_DEFAULT	Yes/No	4	589	592	Is this a default token?
RPKG_UTK_UNKNUSR	Yes/No	4	594	597	Is this an undefined user?
RPKG_UTK_ERROR	Yes/No	4	599	602	Is this user token in error?
RPKG_UTK_TRUSTED	Yes/No	4	604	607	Is this user a part of the TCB?
RPKG_UTK_SESTYPE	Char	8	609	616	The session type of this session.
RPKG_UTK_SURROGAT	Yes/No	4	618	621	Is this a surrogate user?
RPKG_UTK_REMOTE	Yes/No	4	623	626	Is this a remote job?
RPKG_UTK_PRIV	Yes/No	4	628	631	Is this a privileged user ID?
RPKG_UTK_SECL	Char	8	633	640	The SECLABEL of the user.
RPKG_UTK_EXECNODE	Char	8	642	649	The execution node of the work.
RPKG_UTK_SUSER_ID	Char	8	651	658	The submitting user ID.
RPKG_UTK_SNODE	Char	8	660	667	The submitting node.
RPKG_UTK_SGRP_ID	Char	8	669	676	The submitting group name.
RPKG_UTK_SPOE	Char	8	678	685	The port of entry.
RPKG_UTK_SPCLASS	Char	8	687	694	Class of the POE.
RPKG_UTK_USER_ID	Char	8	696	703	User ID associated with the record.
RPKG_UTK_GRP_ID	Char	8	705	712	Group name associated with the record.
RPKG_UTK_DFT_GRP	Yes/No	4	714	717	Is a default group assigned?
RPKG_UTK_DFT_SECL	Yes/No	4	719	722	Is a default SECLABEL assigned?
RPKG_SERIAL_NUMBER	Char	255	724	978	Certificate serial number.
RPKG_ISSUERS_DN	Char	255	980	1234	Certificate issuer's distinguished name.
RPKG_UTK_NETW	Char	8	1236	1243	The port of entry network name.
RPKG_X500_SUBJECT	Char	255	1245	1499	Subject's name associated with this event.
RPKG_X500_ISSUER	Char	255	1501	1755	Issuer's name associated with this event.
RPKG_KEYUSAGE	Char	64	1757	1820	Requested certificate KeyUsage.
RPKG_NOTBEFOR_DATE	Char	10	1822	1831	Requested certificate NotBefore date.

Table 139. Format of the RPKIGENC Record Extension (Event Code 69) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
RPKG_NOTAFTER_DATE	Char	10	1833	1842	Requested certificate NotAfter date.
RPKG_TARGET_USERID	Char	8	1844	1851	IRRSPX00 target User ID.
RPKG_TARGET_LABEL	Char	32	1853	1884	IRRSPX00 target label.
RPKG_SIGNWITH	Char	45	1886	1930	IRRSPX00 SignWith value.
RPKG_SUBJECTS_DN	Char	255	1932	2186	Certificate subject's distinguished name.
RPKG_ALT_IP	Char	64	2188	2251	Requested ALTNAME IP address.
RPKG_ALT_URI	Char	255	2253	2507	Requested ALTNAME URI.
RPKG_ALT_EMAIL	Char	100	2509	2608	Requested ALTNAME EMail.
RPKG_ALT_DOMAIN	Char	100	2610	2709	Requested ALTNAME Domain.
RPKG_CERT_ID	Char	56	2711	2766	IRRSPX00 Certificate ID.
RPKG_HOSTID_MAP	Char	1024	2768	3791	HOSTID mappings extension data.
RPKG_REQUESTOR	Char	32	3793	3824	Requestor's name.
RPKG_PASS_PHRASE	Yes/No	4	3826	3829	Requestor specified a pass phrase.
RPKG_NOTIFY_EMAIL	Char	64	3831	3894	E-mail address for notification purposes.

Event Qualifiers for the RPKIGENC Records

The event qualifiers that may be associated with RPKIGENC records are shown in Table 140.

Table 140. Event Qualifiers for RPKIGENC Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Successful certificate GENCERT request.
INSAUTH	01	Unsuccessful certificate GENCERT request due to insufficient authority.
SUCCESSRQC	02	Successful certificate REQCERT request.
IAUTHRQC	03	Unsuccessful certificate REQCERT request due to insufficient authority.
SUCCESSGMR	04	Successful certificate GENRENEW request.
IAUTHGMR	05	Unsuccessful certificate GENRENEW request due to insufficient authority.
SUCCESSRQR	06	Successful certificate REQRENEW request.
IAUTHRQR	07	Unsuccessful certificate REQRENEW request due to insufficient authority.

The Format of the RPKIEXPT Record Extension

Table 141 describes the format of a record that is created by RPKIEXPT.

Table 141. Format of the RPKIEXPT Record Extension (Event Code 70)

Field Name	Type	Length	Position		Comments
			Start	End	
RPKE_LOGSTRING	Char	255	282	536	Logstring parameter.
RPKE_USER_NAME	Char	20	538	557	The name associated with the user ID.
RPKE_UTK_ENCR	Yes/No	4	559	562	Is the UTKEN associated with this user encrypted?

SMF Data Unload—IRRADU00

Table 141. Format of the RPKIEXPT Record Extension (Event Code 70) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
RPKE_UTK_PRE19	Yes/No	4	564	567	Is this a pre-1.9 token?
RPKE_UTK_VERPROF	Yes/No	4	569	572	Is the VERIFYX propagation.
RPKE_UTK_NJEUNUSR	Yes/No	4	574	577	Is this the NJE undefined user?
RPKE_UTK_LOGUSR	Yes/No	4	579	582	Is UAUDIT specified for this user?
RPKE_UTK_SPECIAL	Yes/No	4	584	587	Is this a SPECIAL user?
RPKE_UTK_DEFAULT	Yes/No	4	589	592	Is this a default token?
RPKE_UTK_UNKNUSR	Yes/No	4	594	597	Is this an undefined user?
RPKE_UTK_ERROR	Yes/No	4	599	602	Is this user token in error?
RPKE_UTK_TRUSTED	Yes/No	4	604	607	Is this user a part of the TCB?
RPKE_UTK_SESSTYPE	Char	8	609	616	The session type of this session.
RPKE_UTK_SURROGAT	Yes/No	4	618	621	Is this a surrogate user?
RPKE_UTK_REMOTE	Yes/No	4	623	626	Is this a remote job?
RPKE_UTK_PRIV	Yes/No	4	628	631	Is this a privileged user ID?
RPKE_UTK_SECL	Char	8	633	640	The SECLABEL of the user.
RPKE_UTK_EXECNODE	Char	8	642	649	The execution node of the work.
RPKE_UTK_SUSER_ID	Char	8	651	658	The submitting user ID.
RPKE_UTK_SNODE	Char	8	660	667	The submitting node.
RPKE_UTK_SGRP_ID	Char	8	669	676	The submitting group name.
RPKE_UTK_SPOE	Char	8	678	685	The port of entry.
RPKE_UTK_SPCLASS	Char	8	687	694	Class of the POE.
RPKE_UTK_USER_ID	Char	8	696	703	User ID associated with the record.
RPKE_UTK_GRP_ID	Char	8	705	712	Group name associated with the record.
RPKE_UTK_DFT_GRP	Yes/No	4	714	717	Is a default group assigned?
RPKE_UTK_DFT_SECL	Yes/No	4	719	722	Is a default SECLABEL assigned?
RPKE_UTK_NETW	Char	8	724	731	The port of entry network name.
RPKE_X500_SUBJECT	Char	255	733	987	Subject's name associated with this event.
RPKE_X500_ISSUER	Char	255	989	1243	Issuer's name associated with this event.
RPKE_TARGET_USERID	Char	8	1245	1252	IRRSPX00 target User ID.
RPKE_TARGET_LABEL	Char	32	1254	1285	IRRSPX00 target label.
RPKE_CERT_ID	Char	56	1287	1342	IRRSPX00 Certificate ID.
RPKE_PASS_PHRASE	Yes/No	4	1344	1347	Requestor specified a pass phrase.

Event Qualifiers for the RPKIEXPT Records

The event qualifiers that may be associated with RPKIEXPT records are shown in Table 142.

Table 142. Event Qualifiers for RPKIEXPT Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESSFUL	00	Successful certificate EXPORT request.
INSAUTH	01	Unsuccessful certificate EXPORT request due to insufficient authority.
INCORPHR	02	Incorrect pass phrase specified for EXPORT

The Format of the Policy Director Authorization Services Support Record Extension

Table 143 describes the format of a record that is created by Policy Director Authorization Services Support.

Table 143. Format of Policy Director Authorization Services Support Record Extension (Event Code 71)

Field Name	Type	Length	Position		Comments
			Start	End	
PDAC_OBJECT	Char	4096	282	4377	The Policy Director Authorization Services Support protected object.
PDAC_REQ_PERMS	Char	1024	4379	5402	The requested Policy Director Authorization Services Support permissions.
PDAC_HOST_USERID	Char	8	5404	5411	The Policy Director Authorization Services Support principal user ID.
PDAC_PRINCIPAL	Char	36	5413	5448	The Policy Director Authorization Services Support principal ID string.
PDAC_QOP	Integer	10	5450	5459	The Policy Director Authorization Services Support quality of protection value.
PDAC_CRED_TYPE	Char	30	5461	5490	The Policy Director Authorization Services Support credential type. The valid types are: "UNAUTHENTICATED" and "AUTHENTICATED"

Event Qualifiers for Policy Director Authorization Services Support Records

The event qualifiers that may be associated with Policy Director Authorization Services Support records are shown in Table 144.

Table 144. Event Qualifiers for Policy Director Authorization Services Support Records

Event Qualifier	Event Qualifier Number	Event Description
AUTH	00	Authorized to access protected object.
UNAUTHW	01	Not authorized to access protected object but permitted because of warning mode.
INSTRAVW	02	Not authorized to access protected object due to insufficient traverse authority but permitted because of warning mode.
TODW	03	Not authorized to access protected object due to time-of-day check but permitted because of warning mode.
UNAUTH	04	Not authorized to access protected object.
INSTRAV	05	Not authorized to access protected object due to insufficient traverse authority.
TOD	06	Not authorized to access protected object due to time-of-day check.

The Format of the RPKIREAD Record Extension

Table 145 describes the format of a record that is created by RPKIREAD.

Table 145. Format of the RPKIREAD Record Extension (Event Code 72)

Field Name	Type	Length	Position		Comments
			Start	End	
RPKR_APPL	Char	8	282	289	Logstring parameter.

SMF Data Unload—IRRADU00

Table 145. Format of the RPKIREAD Record Extension (Event Code 72) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
RPKR_LOGSTRING	Char	255	291	545	Logstring parameter.
RPKR_USER_NAME	Char	20	547	566	The name associated with the user ID.
RPKR_UTK_ENCR	Yes/No	4	568	571	Is the UTOKEN associated with this user encrypted?
RPKR_UTK_PRE19	Yes/No	4	573	576	Is this a pre-1.9 token?
RPKR_UTK_VERPROF	Yes/No	4	578	581	Is the VERIFYX propagation?
RPKR_UTK_NJEUNUSR	Yes/No	4	583	586	Is this the NJE undefined user?
RPKR_UTK_LOGUSR	Yes/No	4	588	591	Is UAUDIT specified for this user?
RPKR_UTK_SPECIAL	Yes/No	4	593	596	Is this a SPECIAL user?
RPKR_UTK_DEFAULT	Yes/No	4	598	601	Is this a default token?
RPKR_UTK_UNKNUSR	Yes/No	4	603	606	Is this an undefined user?
RPKR_UTK_ERROR	Yes/No	4	608	611	Is this user token in error?
RPKR_UTK_TRUSTED	Yes/No	4	613	616	Is this user a part of the TCB?
RPKR_UTK_SESTYPE	Char	8	618	625	The session type of this session.
RPKR_UTK_SURROGAT	Yes/No	4	627	630	Is this a surrogate user?
RPKR_UTK_REMOTE	Yes/No	4	632	635	Is this a remote job?
RPKR_UTK_PRIV	Yes/No	4	637	640	Is this a privileged user ID?
RPKR_UTK_SECL	Char	8	642	649	The SECLABEL of the user.
RPKR_UTK_EXECPNODE	Char	8	651	658	The execution node of the work.
RPKR_UTK_SUSER_ID	Char	8	660	667	The submitting user ID.
RPKR_UTK_SNODE	Char	8	669	676	The submitting node.
RPKR_UTK_SGRP_ID	Char	8	678	685	The submitting group name.
RPKR_UTK_SPOE	Char	8	687	694	The port of entry.
RPKR_UTK_SPCLASS	Char	8	696	703	Class of the POE.
RPKR_UTK_USER_ID	Char	8	705	712	User ID associated with the record.
RPKR_UTK_GRP_ID	Char	8	714	721	Group name associated with the record.
RPKR_UTK_DFT_GRP	Yes/No	4	723	726	Is a default group assigned?
RPKR_UTK_DFT_SECL	Yes/No	4	728	731	Is a default SECLABEL assigned?
RPKR_SERIAL_NUMBER	Char	255	733	987	Certificate serial number.
RPKR_ISSUERS_DN	Char	255	989	1243	Certificate issuer's distinguished name.
RPKR_UTK_NETW	Char	8	1245	1252	The port of entry network name.
RPKR_X500_SUBJECT	Char	255	1254	1508	Subject's name associated with this event.
RPKR_X500_ISSUER	Char	255	1510	1764	Issuer's name associated with this event.
RPKR_KEYUSAGE	Char	64	1766	1829	Requested certificate KeyUsage.
RPKR_NOTBEFOR_DATE	Char	10	1831	1840	Requested certificate NotBefore date.
RPKR_NOTAFTER_DATE	Char	10	1842	1851	Requested certificate NotAfter date.
RPKR_SUBJECTS_DN	Char	255	1853	2107	Certificate subject's distinguished name.
RPKR_CERT_ID	Char	56	2109	2164	IRRSPX00 Certificate ID.
RPKR_REQUESTOR	Char	32	2166	2197	Requestor's name.
RPKR_STATUS	Char	32	2199	2230	Requestor certificate status.
RPKR_CREATION_DATE	Char	10	2232	2241	Requestor certificate creation date (YYYY/MM/DD).
RPKR_LAST_MOD_DATE	Char	10	2243	2252	Requestor certificate last modification date (YYYY/MM/DD).
RPKR_PREV_SERIAL	Char	255	2254	2508	Requestor's previous serial number.

Table 145. Format of the RPKIREAD Record Extension (Event Code 72) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
RPKR_NOTIFY_EMAIL	Char	64	2510	2573	E-mail address for notification purposes.

Event Qualifiers for the RPKIREAD Records

The event qualifiers that may be associated with RPKIREAD records are shown in Table 146.

Table 146. Event Qualifiers for RPKIREAD Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Successful admin QUERY or DETAILS request.
INSAUTH	01	Unsuccessful certificate admin QUERY or DETAILS request due to insufficient authority.
SUCCESSVFY	02	Successful certificate VERIFY request.
IAUTHVFY	03	Unsuccessful certificate VERIFY request due to insufficient authority.
INCORCRT	04	Incorrect VERIFY certificate, no record found for this certificate.

The Format of the RPKIUPDR Record Extension

Table 147 describes the format of a record that is created by RPKIUPDR.

Table 147. Format of the RPKIUPDR Record Extension (Event Code 73)

Field Name	Type	Length	Position		Comments
			Start	End	
RPKU_LOGSTRING	Char	255	282	536	Logstring parameter.
RPKU_USER_NAME	Char	20	538	557	The name associated with the user ID.
RPKU_UTK_ENCR	Yes/No	4	559	562	Is the UTOKEN associated with this user encrypted?
RPKU_UTK_PRE19	Yes/No	4	564	567	Is this a pre-1.9 token?
RPKU_UTK_VERPROF	Yes/No	4	569	572	Is the VERIFYX propagation?
RPKU_UTK_NJEUNUSR	Yes/No	4	574	577	Is this the NJE undefined user?
RPKU_UTK_LOGUSR	Yes/No	4	579	582	Is UAUDIT specified for this user?
RPKU_UTK_SPECIAL	Yes/No	4	584	587	Is this a SPECIAL user?
RPKU_UTK_DEFAULT	Yes/No	4	589	592	Is this a default token?
RPKU_UTK_UNKNUSR	Yes/No	4	594	597	Is this an undefined user?
RPKU_UTK_ERROR	Yes/No	4	599	602	Is this user token in error?
RPKU_UTK_TRUSTED	Yes/No	4	604	607	Is this user a part of the TCB?
RPKU_UTK_SESSTYPE	Char	8	609	616	The session type of this session.
RPKU_UTK_SURROGAT	Yes/No	4	618	621	Is this a surrogate user?
RPKU_UTK_REMOTE	Yes/No	4	623	626	Is this a remote job?
RPKU_UTK_PRIV	Yes/No	4	628	631	Is this a privileged user ID?
RPKU_UTK_SECL	Char	8	633	640	The SECLABEL of the user.
RPKU_UTK_EXECNODE	Char	8	642	649	The execution node of the work.
RPKU_UTK_SUSER_ID	Char	8	651	658	The submitting user ID.

SMF Data Unload—IRRADU00

Table 147. Format of the RPKIUPDR Record Extension (Event Code 73) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
RPKU_UTK_SNODE	Char	8	660	667	The submitting node.
RPKU_UTK_SGRP_ID	Char	8	669	676	The submitting group name.
RPKU_UTK_SPOE	Char	8	678	685	The port of entry.
RPKU_UTK_SPCLASS	Char	8	687	694	Class of the POE.
RPKU_UTK_USER_ID	Char	8	696	703	User ID associated with the record.
RPKU_UTK_GRP_ID	Char	8	705	712	Group name associated with the record.
RPKU_UTK_DFT_GRP	Yes/No	4	714	717	Is a default group assigned?
RPKU_UTK_DFT_SECL	Yes/No	4	719	722	Is a default SECLABEL assigned?
RPKU_UTK_NETW	Char	8	724	731	The port of entry network name.
RPKU_X500_SUBJECT	Char	255	733	987	Subject's name associated with this event.
RPKU_X500_ISSUER	Char	255	989	1243	Issuer's name associated with this event.
RPKU_KEYUSAGE	Char	64	1245	1308	Requested certificate KeyUsage.
RPKU_NOTBEFOR_DATE	Char	10	1310	1319	Requested certificate NotBefore date.
RPKU_NOTAFTER_DATE	Char	10	1321	1330	Requested certificate NotAfter date.
RPKU_SUBJECTS_DN	Char	255	1332	1586	Certificate subject's distinguished name.
RPKU_ALT_IP	Char	64	1588	1651	Requested ALTNAME IP address.
RPKU_ALT_URI	Char	255	1653	1907	Requested ALTNAME URI.
RPKU_ALT_EMAIL	Char	100	1909	2008	Requested ALTNAME EMail.
RPKU_ALT_DOMAIN	Char	100	2010	2109	Requested ALTNAME Domain.
RPKU_CERT_ID	Char	56	2111	2166	IRRSPX00 Certificate ID.
RPKU_HOSTID_MAP	Char	1024	2168	3191	HOSTID mappings extension data.
RPKU_ACTION	Char	16	3193	3208	Action taken against certificate request.
RPKU_ACTION_COM	Char	64	3210	3273	Comment for the action on the certificate request.

Event Qualifiers for the RPKIUPDR Records

The event qualifiers that may be associated with RPKIUPDR records are shown in Table 148.

Table 148. Event Qualifiers for RPKIUPDR Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Successful admin UPDATEREQ request.
INSAUTH	01	Unsuccessful admin UPDATEREQ request due to insufficient authority.

The Format of the RPKIUPDC Record Extension

Table 149 describes the format of a record that is created by RPKIUPDC.

Table 149. Format of the RPKIUPDC Record Extension (Event Code 74)

Field Name	Type	Length	Position		Comments
			Start	End	
RPKC_LOGSTRING	Char	255	282	536	Logstring parameter.
RPKC_USER_NAME	Char	20	538	557	The name associated with the user ID.

Table 149. Format of the RPKIUPDC Record Extension (Event Code 74) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
RPKC_UTK_ENCR	Yes/No	4	559	562	Is the UTKEN associated with this user encrypted?
RPKC_UTK_PRE19	Yes/No	4	564	567	Is this a pre-1.9 token?
RPKC_UTK_VERPROF	Yes/No	4	569	572	Is the VERIFYX propagation?
RPKC_UTK_NJEUNUSR	Yes/No	4	574	577	Is this the NJE undefined user?
RPKC_UTK_LOGUSR	Yes/No	4	579	582	Is UAUDIT specified for this user?
RPKC_UTK_SPECIAL	Yes/No	4	584	587	Is this a SPECIAL user?
RPKC_UTK_DEFAULT	Yes/No	4	589	592	Is this a default token?
RPKC_UTK_UNKNUSR	Yes/No	4	594	597	Is this an undefined user?
RPKC_UTK_ERROR	Yes/No	4	599	602	Is this user token in error?
RPKC_UTK_TRUSTED	Yes/No	4	604	607	Is this user a part of the TCB?
RPKC_UTK_SESTYPE	Char	8	609	616	The session type of this session.
RPKC_UTK_SURROGAT	Yes/No	4	618	621	Is this a surrogate user?
RPKC_UTK_REMOTE	Yes/No	4	623	626	Is this a remote job?
RPKC_UTK_PRIV	Yes/No	4	628	631	Is this a privileged user ID?
RPKC_UTK_SECL	Char	8	633	640	The SECLABEL of the user.
RPKC_UTK_EXECNODE	Char	8	642	649	The execution node of the work.
RPKC_UTK_SUSER_ID	Char	8	651	658	The submitting user ID.
RPKC_UTK_SNODE	Char	8	660	667	The submitting node.
RPKC_UTK_SGRP_ID	Char	8	669	676	The submitting group name.
RPKC_UTK_SPOE	Char	8	678	685	The port of entry.
RPKC_UTK_SPCLASS	Char	8	687	694	Class of the POE.
RPKC_UTK_USER_ID	Char	8	696	703	User ID associated with the record.
RPKC_UTK_GRP_ID	Char	8	705	712	Group name associated with the record.
RPKC_UTK_DFT_GRP	Yes/No	4	714	717	Is a default group assigned?
RPKC_UTK_DFT_SECL	Yes/No	4	719	722	Is a default SECLABEL assigned?
RPKC_SERIAL_NUMBER	Char	255	724	978	Certificate serial number.
RPKC_UTK_NETW	Char	8	980	987	The port of entry network name.
RPKC_X500_SUBJECT	Char	255	989	1243	Subject's name associated with this event.
RPKC_X500_ISSUER	Char	255	1245	1499	Issuer's name associated with this event.
RPKC_ACTION	Char	16	1501	1516	Action taken against certificate request.
RPKC_ACTION_COM	Char	64	1518	1581	Comment for the certificate request.
RPKC_REVOKE_RSN	Char	32	1583	1614	Reason for certificate revocation.

Event Qualifiers for the RPKIUPDC Records

The event qualifiers that may be associated with RPKIUPDC records are shown in Table 150.

Table 150. Event Qualifiers for RPKIUPDC Records

Event Qualifier	Event Qualifier Number	Event Description
SUCCESS	00	Successful admin UPDATECERT request.
INSAUTH	01	Unsuccessful admin UPDATECERT request due to insufficient authority.

SMF Data Unload—IRRADU00

Table 150. Event Qualifiers for RPKIUPDC Records (continued)

Event Qualifier	Event Qualifier Number	Event Description
SUCCSRVK	02	Successful certificate REVOKE request.
IAUTHRVK	03	Unsuccessful certificate REVOKE request due to insufficient authority.

The Format of the SETFACL Record Extension

Table 151 describes the format of a record that is created by adding, modifying, or deleting an access control list entry of a z/OS UNIX file.

Table 151. Format of the SETFACL Record Extension (Event Code 75)

Field Name	Type	Length	Position		Comments
			Start	End	
SACL_CLASS	Char	8	282	289	Class name.
SACL_USER_NAME	Char	20	291	310	The name associated with the user ID.
SACL_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
SACL_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
SACL_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
SACL_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
SACL_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
SACL_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
SACL_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
SACL_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
SACL_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
SACL_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
SACL_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
SACL_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
SACL_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
SACL_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
SACL_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
SACL_UTK_EXECNODE	Char	8	395	402	The execution node of the work.
SACL_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
SACL_UTK_SNODE	Char	8	413	420	The submitting node.
SACL_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
SACL_UTK_SPOE	Char	8	431	438	The port of entry.
SACL_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
SACL_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
SACL_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
SACL_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
SACL_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
SACL_APPC_LINK	Char	16	477	492	Key to link together APPC records.
SACL_AUDIT_CODE	Char	11	494	504	Audit function code.
SACL_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
SACL_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).

Table 151. Format of the SETFACL Record Extension (Event Code 75) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
SACL_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
SACL_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
SACL_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
SACL_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
SACL_PATH_NAME	Char	1023	572	1594	The requested path name.
SACL_FILE_ID	Char	32	1596	1627	File ID.
SACL_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
SACL_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
SACL_FILEPOOL	Char	8	1651	1658	SFS filepool containing the BFS file.
SACL_FILESPEACE	Char	8	1660	1667	SFS filespace containing the BFS file.
SACL_INODE	Integer	10	1669	1678	Inode (file serial number)
SACL_SCID	Integer	10	1680	1689	File SCID
SACL_DCE_LINK	Char	16	1691	1706	Link to connect DCE records that originate from a DCE request
SACL_AUTH_TYPE	Char	13	1708	1720	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
SACL_DFLT_PROCESS	Yes/No	4	1722	1725	Default z/OS UNIX security environment in effect
SACL_UTK_NETW	Char	8	1727	1734	Port of entry network name
SACL_X500_SUBJECT	Char	255	1736	1990	Subject's name associated with this request.
SACL_X500_ISSUER	Char	255	1992	2246	Issuer's name associated with this request
SACL_ACL_TYPE	Char	8	2248	2255	What type of ACL is this? Valid values are "ACCESS", "FILEMOD", and "DIRMOD".
SACL_OPTYPE	Char	8	2257	2264	ACL entry operation. Valid values are "ADD", "MODIFY", and "DELETE".
SACL_ENTRY_TYPE	Char	3	2266	2268	ACL entry type. Valid values are "UID" and "GID".
SACL_ENTRY_ID	Integer	10	2270	2279	UID or GID value in the ACL entry.
SACL_OLD_READ	Yes/No	4	2281	2284	Was the READ bit on for this entry? (blank when SACL_OPTYPE is ADD)
SACL_OLD_WRITE	Yes/No	4	2286	2289	Was the WRITE bit on for this entry? (blank when SACL_OPTYPE is ADD)
SACL_OLD_EXECUTE	Yes/No	4	2291	2294	Was the EXECUTE bit on for this entry? (blank when SACL_OPTYPE is ADD)
SACL_NEW_READ	Yes/No	4	2296	2299	Was the READ bit on for this entry? (blank when SACL_OPTYPE is DELETE)
SACL_NEW_WRITE	Yes/No	4	2301	2304	Was the WRITE bit on for this entry? (blank when SACL_OPTYPE is DELETE)
SACL_NEW_EXECUTE	Yes/No	4	2306	2309	Was the EXECUTE bit on for this entry? (blank when SACL_OPTYPE is DELETE)

Event Qualifiers for SETFACL Records

The event qualifiers that may be associated with an access control list modification event are shown in Table 152 on page 238.

SMF Data Unload—IRRADU00

Table 152. Event Qualifiers for SETFACL Records

Event Qualifier	Event Qualifier Number	Event Description
	00	ACL entry added, modified, or deleted.
	01	Caller does not have authority to change ACL of the specified file.

The Format of the DELFACL Record Extension

Table 153 describes the format of a record that is created by deleting an access control list of a z/OS UNIX file.

Table 153. Format of the DELFACL Record Extension (Event Code 76)

Field Name	Type	Length	Position		Comments
			Start	End	
DACL_CLASS	Char	8	282	289	Class name.
DACL_USER_NAME	Char	20	291	310	The name associated with the user ID.
DACL_UTK_ENCR	Yes/No	4	312	315	Is the UTOKEN associated with this user encrypted?
DACL_UTK_PRE19	Yes/No	4	317	320	Is this a pre-1.9 token?
DACL_UTK_VERPROF	Yes/No	4	322	325	Is the VERIFYX propagation flag set?
DACL_UTK_NJEUNUSR	Yes/No	4	327	330	Is this the NJE undefined user?
DACL_UTK_LOGUSR	Yes/No	4	332	335	Is UAUDIT specified for this user?
DACL_UTK_SPECIAL	Yes/No	4	337	340	Is this a SPECIAL user?
DACL_UTK_DEFAULT	Yes/No	4	342	345	Is this a default token?
DACL_UTK_UNKNUSR	Yes/No	4	347	350	Is this an undefined user?
DACL_UTK_ERROR	Yes/No	4	352	355	Is this user token in error?
DACL_UTK_TRUSTED	Yes/No	4	357	360	Is this user a part of the trusted computing base (TCB)?
DACL_UTK_SESSTYPE	Char	8	362	369	The session type of this session.
DACL_UTK_SURROGAT	Yes/No	4	371	374	Is this a surrogate user?
DACL_UTK_REMOTE	Yes/No	4	376	379	Is this a remote job?
DACL_UTK_PRIV	Yes/No	4	381	384	Is this a privileged user ID?
DACL_UTK_SECL	Char	8	386	393	The SECLABEL of the user.
DACL_UTK_EXECPNODE	Char	8	395	402	The execution node of the work.
DACL_UTK_SUSER_ID	Char	8	404	411	The submitting user ID.
DACL_UTK_SNODE	Char	8	413	420	The submitting node.
DACL_UTK_SGRP_ID	Char	8	422	429	The submitting group name.
DACL_UTK_SPOE	Char	8	431	438	The port of entry.
DACL_UTK_SPCLASS	Char	8	440	447	Class of the POE. Valid values are "TERMINAL", "CONSOLE", "JESINPUT", and "APPCPORT".
DACL_UTK_USER_ID	Char	8	449	456	User ID associated with the record.
DACL_UTK_GRP_ID	Char	8	458	465	Group name associated with the record.
DACL_UTK_DFT_GRP	Yes/No	4	467	470	Is a default group assigned?
DACL_UTK_DFT_SECL	Yes/No	4	472	475	Is a default SECLABEL assigned?
DACL_APPC_LINK	Char	16	477	492	Key to link together APPC records.
DACL_AUDIT_CODE	Char	11	494	504	Audit function code.
DACL_OLD_REAL_UID	Integer	10	506	515	Old real z/OS UNIX user identifier (UID).
DACL_OLD_EFF_UID	Integer	10	517	526	Old effective z/OS UNIX user identifier (UID).

Table 153. Format of the DELFACL Record Extension (Event Code 76) (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
DACL_OLD_SAVED_UID	Integer	10	528	537	Old saved z/OS UNIX user identifier (UID).
DACL_OLD_REAL_GID	Integer	10	539	548	Old real z/OS UNIX group identifier (GID).
DACL_OLD_EFF_GID	Integer	10	550	559	Old effective z/OS UNIX group identifier (GID).
DACL_OLD_SAVED_GID	Integer	10	561	570	Old saved z/OS UNIX group identifier (GID).
DACL_PATH_NAME	Char	1023	572	1594	The requested path name.
DACL_FILE_ID	Char	32	1596	1627	File ID.
DACL_FILE_OWN_UID	Integer	10	1629	1638	The owner z/OS UNIX user identifier (UID) associated with the file.
DACL_FILE_OWN_GID	Integer	10	1640	1649	The owner z/OS UNIX group identifier (GID) associated with the file.
DACL_FILEPOOL	Char	8	1651	1658	SFS filepool containing the BFS file.
DACL_FILESPACE	Char	8	1660	1667	SFS filespace containing the BFS file.
DACL_INODE	Integer	10	1669	1678	Inode (file serial number)
DACL_SCID	Integer	10	1680	1689	File SCID
DACL_DCE_LINK	Char	16	1691	1706	Link to connect DCE records that originate from a DCE request
DACL_AUTH_TYPE	Char	13	1708	1720	Defines the type of request. Valid values are: "SERVER", "AUTH_CLIENT", and "UNAUTH_CLIENT".
DACL_DFLT_PROCESS	Yes/No	4	1722	1725	Default z/OS UNIX security environment in effect
DACL_UTK_NETW	Char	8	1727	1734	Port of entry network name
DACL_X500_SUBJECT	Char	255	1736	1990	Subject's name associated with this request.
DACL_X500_ISSUER	Char	255	1992	2246	Issuer's name associated with this request
DACL_ACL_TYPE	Char	8	2248	2255	What type of ACL is this? Valid values are "ACCESS", "FILEMOD", and "DIRMOD".

Event Qualifiers for DELFACL Records

The event qualifiers that may be associated with an access control list deletion event are shown in Table 154.

Table 154. Event Qualifiers for DELFACL Records

Event Qualifier	Event Qualifier Number	Event Description
	00	Entire ACL removed.
	01	Caller does not have authority to remove ACL of the specified file.

SMF Data Unload—IRRADU00

Chapter 7. The Format of the Unloaded SMF Type 81 Data

RACF writes a type 81 record at the completion of the initialization of RACF. Table 155 describes the format of the unloaded version of this record.

Table 155. Format of the Unloaded SMF Type 81 Records

Field Name	Type	Length	Position		Comments
			Start	End	
RINI_EVENT_TYPE	Char	8	1	8	The type of the event. Set to "RACFINIT".
RINI_RESERVED_01	Char	8	10	17	This field is reserved and is set to blanks to allow a common alignment with other unloaded SMF records.
RINI_TIME_WRITTEN	Time	8	19	26	Time that the record was written to SMF.
RINI_DATE_WRITTEN	Date	10	28	37	Date that the record was written to SMF.
RINI_SYSTEM_SMFID	Char	4	39	42	SMF system ID of the system from which the record originates.
RINI_DATASET_NAME	Char	44	44	87	Name of the RACF database for this IPL.
RINI_DATASET_VOL	Char	6	89	94	Volume upon which the RACF data set resides
RINI_DATASET_UNIT	Char	3	96	98	Unit name of the RACF database.
RINI_UADS_NAME	Char	44	100	143	Name of the user attribute data set for this IPL.
RINI_UADS_VOL	Char	6	145	150	Volume upon which the user attribute data set resides.
RINI_RACINIT_STATS	Yes/No	4	152	155	Are RACINIT statistics recorded?
RINI_DATASET_STATS	Yes/No	4	157	160	Are data set statistics recorded?
RINI_RACINIT_PRE	Yes/No	4	162	165	Is there a RACROUTE REQUEST=VERIFY preprocessing exit (ICHRIX01)?
RINI_RACHECK_PRE	Yes/No	4	167	170	Is there a RACROUTE REQUEST=AUTH preprocessing exit (ICHRCX01)?
RINI_RACDEF_PRE	Yes/No	4	172	175	Is there a RACROUTE REQUEST=DEFINE preprocessing exit (ICHRDX01)?
RINI_RACINIT_POST	Yes/No	4	177	180	Is there a RACROUTE REQUEST=VERIFY postprocessing exit (ICHRIX02)?
RINI_RACHECK_POST	Yes/No	4	182	185	Is there a RACROUTE REQUEST=AUTH postprocessing exit (ICHRCX02)?
RINI_NEW_PWD_EXIT	Yes/No	4	187	190	Is there a new password exit routine (ICHPWX01)?
RINI_TAPEVOL_STATS	Yes/No	4	192	195	Are tape volume statistics recorded?
RINI_DASD_STATS	Yes/No	4	197	200	Are DASD statistics recorded?
RINI_TERM_STATS	Yes/No	4	202	205	Are terminal statistics recorded?
RINI_CMD_EXIT	Yes/No	4	207	210	Is the command exit routine ICHCNX00 active? ICHCNX00 is invoked for RACF commands, the IRRUT100 utility, and by IRRXT00 when a RACROUTE REQUEST=EXTRACT is issued for CLASS=DATASET.
RINI_DEL_CMD_EXIT	Yes/No	4	212	215	Is the command exit routine ICHCCX00 active? ICHCCX00 is invoked for the DELGROUP, DELUSER, and REMOVE commands.
RINI_ADSP	Yes/No	4	217	220	Is ADSP active?
RINI_ENCRYPT_EXIT	Yes/No	4	222	225	Is the encryption exit ICHDEX01 active?
RINI_NAMING_CONV	Yes/No	4	227	230	Is the naming convention table ICHNCV00 present?
RINI_TAPEVOL	Yes/No	4	232	235	Is tape volume protection in effect?

Table 155. Format of the Unloaded SMF Type 81 Records (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
RINI_DUP_DSNS	Yes/No	4	237	240	Are duplicate data set names allowed to be defined?
RINI_DASD	Yes/No	4	242	245	Is DASD volume protection in effect?
RINI_FRACHECK_PRE	Yes/No	4	247	250	Is the RACROUTE REQUEST=FASTAUTH preprocessing exit (ICHRFX01) active?
RINI_RACLIST_PRE	Yes/No	4	252	255	Is the RACROUTE REQUEST=LIST pre/postprocessing exit (ICHRFX01) active?
RINI_RACLIST_SEL	Yes/No	4	257	260	Is the RACROUTE REQUEST=LIST selection exit (ICHRFX02) active?
RINI_RACDEF_POST	Yes/No	4	262	265	Is the RACROUTE REQUEST=DEFINE postprocessing exit (ICHRDX02) active?
RINI_AUDIT_USER	Yes/No	4	267	270	Are user class profile changes being audited?
RINI_AUDIT_GROUP	Yes/No	4	272	275	Are group class profile changes being audited?
RINI_AUDIT_DATASET	Yes/No	4	277	280	Are data set class profile changes being audited?
RINI_AUDIT_TAPEVOL	Yes/No	4	282	285	Are tape volume class profile changes being audited?
RINI_AUDIT_DASDVOL	Yes/No	4	287	290	Are DASD volume class profile changes being audited?
RINI_AUDIT_TERM	Yes/No	4	292	295	Are terminal class profile changes being audited?
RINI_AUDIT_CMDVIOL	Yes/No	4	297	300	Are command violations being audited?
RINI_AUDIT_SPECIAL	Yes/No	4	302	305	Are special users being audited?
RINI_AUDIT_OPER	Yes/No	4	307	310	Are operations users being audited?
RINI_AUDIT_LEVEL	Yes/No	4	312	315	Is auditing by security level in effect?
RINI_ACEE_COMPRESS	Yes/No	4	317	320	Is the IRRACX01 exit in effect?
RINI_FASTAUTH_PRE	Yes/No	4	322	325	Is the FASTAUTH AR mode preprocessing exit (ICHRFX03) in effect?
RINI_FASTAUTH_POST	Yes/No	4	327	330	Is the FASTAUTH AR mode postprocessing exit (ICHRFX04) in effect?
RINI_TERM	Yes/No	4	332	335	Is terminal authorization checking in effect?
RINI_TERM_NONE	Yes/No	4	337	340	Are undefined terminals treated as UACC=NONE?
RINI_REALDSN	Yes/No	4	342	345	Is REALDSN in effect?
RINI_XBMALLRACF	Yes/No	4	347	350	Is the JES XBMALLRACF option in effect?
RINI_EARLYVERIFY	Yes/No	4	352	355	Is the JES EARLYVERIFY option in effect?
RINI_BATCHALLRACF	Yes/No	4	357	360	Is the JES BATCHALLRACF option in effect?
RINI_FRACHECK_POST	Yes/No	4	362	365	Is the RACROUTE REQUEST=FASTAUTH post processing exit (ICHRFX02) in effect?
RINI_PWD_INT	Integer	3	367	369	The maximum password interval.
RINI_SINGLE_DSN	Char	8	371	378	The single level data set name.
RINI_TAPEDSN	Yes/No	4	380	383	Is TAPEDSN in effect?
RINI_PROTECTALL	Yes/No	4	385	388	Is PROTECTALL in effect?
RINI_PROTECTALL_W	Yes/No	4	390	393	Is PROTECTALL warning in effect?
RINI_ERASE	Yes/No	4	395	398	Is ERASE-ON-SCRATCH in effect?
RINI_ERASE_LEVEL	Yes/No	4	400	403	Is ERASE-ON-SCRATCH based on security level in effect?
RINI_ERASE_ALL	Yes/No	4	405	408	Is ERASE-ON-SCRATCH for all data sets in effect?
RINI_EGN	Yes/No	4	410	413	Is enhanced generic naming in effect?

Table 155. Format of the Unloaded SMF Type 81 Records (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
RINI_WHEN_PROGRAM	Yes/No	4	415	418	Is access control by program in effect?
RINI_RETENTION	Integer	5	420	424	System retention period.
RINI_LEVEL_ERASE	Integer	5	426	430	Security level for ERASE-ON-SCRATCH.
RINI_LEVEL_AUDIT	Integer	5	432	436	Security level for auditing.
RINI_SECL_CTRL	Yes/No	4	438	441	Is SECLABELCONTROL in effect?
RINI_CATDSNS	Yes/No	4	443	446	Is CATDSNS in effect?
RINI_MLQUIET	Yes/No	4	448	451	Is MLQUIET in effect?
RINI_MLSTABLE	Yes/No	4	453	456	Is MLSTABLE in effect?
RINI_MLS	Yes/No	4	458	461	Is MLS in effect?
RINI_MLACTIVE	Yes/No	4	463	466	Is MLACTIVE in effect?
RINI_GENERIC_OWNER	Yes/No	4	468	471	Is GENERICOWNER in effect?
RINI_SECL_AUDIT	Yes/No	4	473	476	Is SECLABELAUDIT in effect?
RINI_SESSION_INT	Integer	5	478	482	Partner LU-verification session key interval.
RINI_NJE_NAME_ID	Char	8	484	491	JES NJE name user ID.
RINI_NJE_UDFND_ID	Char	8	493	500	JES UNDEFINEDUSER user ID.
RINI_COMPATMODE	Yes/No	4	502	505	Is COMPATMODE in effect?
RINI_CATDSNS_FAIL	Yes/No	4	507	510	Is CATDSNS failures in effect?
RINI_MLS_FAIL	Yes/No	4	512	515	Is MLS failures in effect?
RINI_MLACTIVE_FAIL	Yes/No	4	517	520	Is MLACTIVE failures in effect?
RINI_APPLAUD	Yes/No	4	522	525	Is APPLAUDIT in effect?
RINI_DFT_PRI	Char	3	527	529	Default primary language for the installation.
RINI_DFT_SEC	Char	3	531	533	Default secondary language for the installation.
RINI_RESERVED_02	Char	4	535	538	Reserved
RINI_ALL_CMD_EXIT	Yes/No	4	540	543	Did the exit for all commands (IRREVSX01) have any active exit routines at IPL time?
RINI_ADDCREATOR	Yes/No	4	545	548	Is the SETROPTS ADDCREATOR option in effect?
RINI_ACEE_COMP_XM	Yes/No	4	550	553	Is the IRRACX02 exit in effect?
RINI_ENCRYPT_EXIT2	Yes/No	4	555	558	Is IRRDEX11 exit in effect?
RINI_PWD_HIST	Integer	3	560	562	The password history value.
RINI_PWD_REVOKE	Integer	3	564	566	The number of incorrect logon passwords before users are revoked.
RINI_PWD_WARN	Integer	3	568	570	The number of days before password expiry during which users receive a warning message.
RINI_PWDRULE1_MIN	Integer	1	572	572	Password syntax rule 1 minimum length.
RINI_PWDRULE1_MAX	Integer	1	574	574	Password syntax rule 1 maximum length.
RINI_PWDRULE1	Char	8	576	583	Password syntax rule 1.
RINI_PWDRULE2_MIN	Integer	1	585	585	Password syntax rule 2 minimum length.
RINI_PWDRULE2_MAX	Integer	1	587	587	Password syntax rule 2 maximum length.
RINI_PWDRULE2	Char	8	589	596	Password syntax rule 2.
RINI_PWDRULE3_MIN	Integer	1	598	598	Password syntax rule 3 minimum length.
RINI_PWDRULE3_MAX	Integer	1	600	600	Password syntax rule 3 maximum length.
RINI_PWDRULE3	Char	8	602	609	Password syntax rule 3.
RINI_PWDRULE4_MIN	Integer	1	611	611	Password syntax rule 4 minimum length.
RINI_PWDRULE4_MAX	Integer	1	613	613	Password syntax rule 4 maximum length.

Table 155. Format of the Unloaded SMF Type 81 Records (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
RINI_PWDRULE4	Char	8	615	622	Password syntax rule 4.
RINI_PWDRULE5_MIN	Integer	1	624	624	Password syntax rule 5 minimum length.
RINI_PWDRULE5_MAX	Integer	1	626	626	Password syntax rule 5 maximum length.
RINI_PWDRULE5	Char	8	628	635	Password syntax rule 5.
RINI_PWDRULE6_MIN	Integer	1	637	637	Password syntax rule 6 minimum length.
RINI_PWDRULE6_MAX	Integer	1	639	639	Password syntax rule 6 maximum length.
RINI_PWDRULE6	Char	8	641	648	Password syntax rule 6.
RINI_PWDRULE7_MIN	Integer	1	650	650	Password syntax rule 7 minimum length.
RINI_PWDRULE7_MAX	Integer	1	652	652	Password syntax rule 7 maximum length.
RINI_PWDRULE7	Char	8	654	661	Password syntax rule 7.
RINI_PWDRULE8_MIN	Integer	1	663	663	Password syntax rule 8 minimum length.
RINI_PWDRULE8_MAX	Integer	1	665	665	Password syntax rule 8 maximum length.
RINI_PWDRULE8	Char	8	667	674	Password syntax rule 8.
RINI_INACTIVE	Integer	3	676	678	The number of days of inactivity before users are revoked.
RINI_GRPLIST	Yes/No	4	680	683	Is list-of-groups processing in effect?
RINI_MOD_GDG	Yes/No	4	685	688	Is MODEL(GDG) in effect?
RINI_MOD_USER	Yes/No	4	690	693	Is MODEL(USER) in effect?
RINI_MOD_GROUP	Yes/No	4	695	698	Is MODEL(GROUP) in effect?
RINI_RSWI_INST_PWD	Yes/No	4	700	703	"Yes" if an installation-defined RVARY SWITCH password is in effect. "No" if the default RVARY SWITCH password is in effect.
RINI_RSTA_INST_PWD	Yes/No	4	705	708	"Yes" if an installation-defined RVARY STATUS password is in effect. "No" if the default RVARY STATUS password is in effect.
RINI_KERBLVL	Char	4	710	713	Level of KERB segment processing in effect.

Chapter 8. The Format of the Unloaded SMF Type 81 Class Data

Table 156 describes the format of the class information that is contained in the SMF type 81 record.

Table 156. Format of the Unloaded SMF Type 81 Class Records

Field Name	Type	Length	Position		Comments
			Start	End	
RINC_EVENT_TYPE	Char	8	1	8	The type of the event. Set to "CLASNAME".
RINC_RESERVED_01	Char	8	10	17	This field is reserved and is set to blanks to allow a common alignment with other unloaded SMF records.
RINC_TIME_WRITTEN	Time	8	19	26	Time that the record was written to SMF.
RINC_DATE_WRITTEN	Date	10	28	37	Date that the record was written to SMF.
RINC_SYSTEM_SMFID	Char	4	39	42	SMF system ID of the system from which the record originates.
RINC_CLASS_NAME	Char	8	44	51	The name of the class.
RINC_STATS	Yes/No	4	53	56	Are statistics collected for this class?
RINC_AUDIT	Yes/No	4	58	61	Is this class being audited?
RINC_ACTIVE	Yes/No	4	63	66	Is this class active?
RINC_GENERIC	Yes/No	4	68	71	May generic profiles be defined in this class?
RINC_GENCMD	Yes/No	4	73	76	Is generic command processing enabled for this class?
RINC_GLOBAL	Yes/No	4	78	81	Is this class enabled for global access checking?
RINC_RACLIST	Yes/No	4	83	86	May SETR RACLIST be issued for this class?
RINC_GENLIST	Yes/No	4	88	91	May SETR GENLIST be issued for this class?
RINC_LOG_OPTIONS	Char	8	93	100	The LOGOPTIONS for the class. Valid values are "ALWAYS", "NEVER", "SUCCESS", "FAILURES", and "DEFAULT".

Chapter 9. The Format of the Unloaded SMF Type 83 Data

RACF writes a type 83 record for each data set that is affected by the change of a SECLABEL. Table 157 describes the format of the unloaded version of this record.

Table 157. Format of the Unloaded SMF Type 83 Records

Field Name	Type	Length	Position		Comments
			Start	End	
DSAF_EVENT_TYPE	Char	8	1	8	The type of the event. Set to "DSAF".
DSAF_RESERVED_01	Char	8	10	17	This field is reserved and is set to blanks to allow a common alignment with other unloaded SMF records.
DSAF_TIME_WRITTEN	Time	8	19	26	Time that the record was written to SMF.
DSAF_DATE_WRITTEN	Date	10	28	37	Date that the record was written to SMF.
DSAF_SYSTEM_SMFID	Char	4	39	42	SMF system ID of the system from which the record originates.
DSAF_SECL_LINK	Char	16	44	59	Key to link together the data sets affected by a change of SECLABEL and the command that caused the SECLABEL change.
DSAF_VIOLATION	Yes/No	4	61	64	Does this record represent a violation?
DSAF_USER_NDFND	Yes/No	4	66	69	Was this user not defined to RACF?
DSAF_USER_WARNING	Yes/No	4	71	74	Was this record created because of WARNING?
DSAF_EVT_USER_ID	Char	8	76	83	User ID associated with the event.
DSAF_EVT_GRP_ID	Char	8	85	92	Group name associated with the event.
DSAF_AUTH_NORMAL	Yes/No	4	94	97	Was normal authority checking a reason for access being allowed?
DSAF_AUTH_SPECIAL	Yes/No	4	99	102	Was special authority checking a reason for access being allowed?
DSAF_AUTH_OPER	Yes/No	4	104	107	Was operations authority checking a reason for access being allowed?
DSAF_AUTH_AUDIT	Yes/No	4	109	112	Was auditor authority checking a reason for access being allowed?
DSAF_AUTH_EXIT	Yes/No	4	114	117	Was exit checking a reason for access being allowed?
DSAF_AUTH_FAILSFT	Yes/No	4	119	122	Was failsoft checking a reason for access being allowed?
DSAF_AUTH_BYPASS	Yes/No	4	124	127	Was the use of the user ID *BYPASS* a reason for access being allowed?
DSAF_AUTH_TRUSTED	Yes/No	4	129	132	Was trusted authority checking a reason for access being allowed?
DSAF_LOG_CLASS	Yes/No	4	134	137	Was SETR AUDIT(class) checking a reason for this event to be recorded?
DSAF_LOG_USER	Yes/No	4	139	142	Was auditing requested for this user?
DSAF_LOG_SPECIAL	Yes/No	4	144	147	Was auditing requested for access granted due to the SPECIAL privilege?
DSAF_LOG_ACCESS	Yes/No	4	149	152	Did the profile indicate audit, or did FAILSOFT processing allow access, or did the RACHECK exit indicate auditing?
DSAF_LOG_RACINIT	Yes/No	4	154	157	Did the RACINIT fail?
DSAF_LOG_ALWAYS	Yes/No	4	159	162	Is this command always audited?
DSAF_LOG_CMDVIOL	Yes/No	4	164	167	Was this event audited due to CMDVIOL?
DSAF_LOG_GLOBAL	Yes/No	4	169	172	Was this event audited due to GLOBALAUDIT?

Table 157. Format of the Unloaded SMF Type 83 Records (continued)

Field Name	Type	Length	Position		Comments
			Start	End	
DSAF_TERM_LEVEL	Integer	3	174	176	The terminal level associated with this audit record.
DSAF_BACKOUT_FAIL	Yes/No	4	178	181	Did RACF fail in backing out the data?
DSAF_PROF_SAME	Yes/No	4	183	186	Was the profile the same at the end of this event?
DSAF_TERM	Char	8	188	195	The terminal associated with the event.
DSAF_JOB_NAME	Char	8	197	204	The job name associated with the event.
DSAF_READ_TIME	Time	8	206	213	The time that the job entered the system.
DSAF_READ_DATE	Date	10	215	224	The date that the job entered the system.
DSAF_SMF_USER_ID	Char	8	226	233	User ID from SMF common area. This value is managed by SMF and the SMF processing exits.
DSAF_LOG_LEVEL	Yes/No	4	235	238	Was this event audited due to SECLEVEL auditing?
DSAF_LOG_LOGOPT	Yes/No	4	240	243	Was this event audited due to SETR LOGOPTIONS auditing?
DSAF_LOG_SECL	Yes/No	4	245	248	Was this event audited due to SETR SECLABELAUDIT auditing?
DSAF_LOG_COMPATM	Yes/No	4	250	253	Was this event audited due to SETR COMPATMODE auditing?
DSAF_LOG_APPLAUD	Yes/No	4	255	258	Was this event audited due to SETR APPLAUDIT?
DSAF_USR_SECL	Char	8	260	267	The SECLABEL associated with this user.
DSAF_DATA_SET	Char	44	269	312	The name of the data set affected by the SECLABEL change.

Chapter 10. RACF Database Unload Utility (IRRDBU00)

Running the Unload

Whenever you need to run the database unload utility against a database that is active on a system that is a member of the RACF sysplex data sharing group, always run the utility from a system in the group. If you do not, you may receive unpredictable results from the utility.

IRRDBU00 Record Types

The database unload utility gives every record it creates a record type. This record type is a 4-byte identification number located in the first four positions of every record.

The record types and their associated names are:

Record Type	Record Name
0100	Group Basic Data
0101	Group Subgroups
0102	Group Members
0103	Group Installation Data
0110	Group DFP Data
0120	Group OMVS Data
0130	Group OVM Data
0140	Reserved
0141	Group TME Data
0200	User Basic Data
0201	User Categories
0202	User Classes
0203	User Group Connections
0204	User Installation Data
0205	User Connect Data
0206	User RRSF Data
0207	User Certificate Name
0208	User Associated Mappings Record
0210	User DFP Data
0220	User TSO Data
0230	User CICS Data
0231	User CICS Operator Classes
0240	User Language Data
0250	User OPERPARM Data
0251	User OPERPARM Scope
0260	User WORKATTR Data
0270	User OMVS Data
0280	User NETVIEW Segment
0281	User OPCLASS
0282	User DOMAINS
0290	User DCE Data
02A0	User OVM Data
02B0	User LNOTES Data
02C0	User NDS Data
02D0	User KERB Data
02E0	User PROXY Data

Database Unload—IRRDBU00

I	02F0	User EIM Data Record
	0400	Data Set Basic Data
	0401	Data Set Categories
	0402	Data Set Conditional Access
	0403	Data Set Volumes
	0404	Data Set Access
	0405	Data Set Installation Data
	0410	Data Set DFP Data
	0420	Reserved
	0421	Data Set TME Data
	0500	General Resource Basic Data
	0501	General Resource Tape Volume Data
	0502	General Resource Categories
	0503	General Resource Members
	0504	General Resource Volumes
	0505	General Resource Access
	0506	General Resource Installation Data
	0507	General Resource Conditional Access
	0508	Filter Data Record
	0510	General Resource Session Data
	0511	General Resource Session Entities
	0520	General Resource DLF Data
	0521	General Resource DLF Job Names
	0530	Reserved
	0540	General Resource Started Task Data
	0550	General Resource SystemView Data
	0560	General Resource Certificate Data Record
	0561	General Resource Certificate References Record
	0562	General Resource Key Ring Data Record
	0570	General Resource TME Data Record
	0571	General Resource TME Child Record
	0572	General Resource TME Resource Record
	0573	General Resource TME Group Record
	0574	General Resource TME Role Record
	0580	General Resource KERB Data
	0590	General Resource PROXY Data
I	05A0	General Resource EIM Data

The record type identification number is in the format **PPSF**, where

PP	Profile type
01	For groups
02	For users
04	For data sets
05	For general resources
S	Segment number
0	Base segment
all others	Segment value determined by the position of the segment in the template
F	Repeat group within the segment. A zero (0) indicates the non-repeat groups within a segment.

The Relationships among Unloaded Database Records

The following figures describe how the records produced by the database unload utility relate to each other. The conventions used in the figures are:

- Only fields showing a relationship to another record type are described
- A line shows a relationship between different types of records
- The complete field names are in the format

prefix_fieldname

where *prefix* is the unique record prefix assigned to the record and *fieldname* identifies the field in the record. Each section provides the prefix added to the field names.

- The arrows on the connecting line clarify the relationship; they point to the field that had to have existed first in the RACF database.

For example, there is a user named GARREN. GARREN creates a group named TEST. The user ID named GARREN had to exist before the group TEST was created.

In terms of the output from database unload, there exists a user basic data record with GARREN in the USBD_NAME field. There also exists a group basic data record with TEST in the GPBD_NAME field and GARREN in the GPBD_OWNER_ID field.

The figures illustrating the relationships are located as follows:

- Group records, see Figure 1 on page 252
- User records, see Figure 3 on page 254
- Data Set records, see Figure 4 on page 255
- General Resource records, see Figure 5 on page 257.

Group Records

The prefix representing the record identifier is omitted in the pictorial diagrams. For group records, the prefixes are:

Record Name	Record Type	Record Prefix
Group Basic Data	0100	GPBD
Group Subgroups	0101	GPSGRP
Group Members	0102	GPMEM
Group Installation Data	0103	GPINSTD
Group DFP Data	0110	GPDFP
Group OMVS Data	0120	GPOMVS
Group OVM Data	0130	GPOVM
Group TME Data	0141	GPTME

Database Unload—IRRDBU00

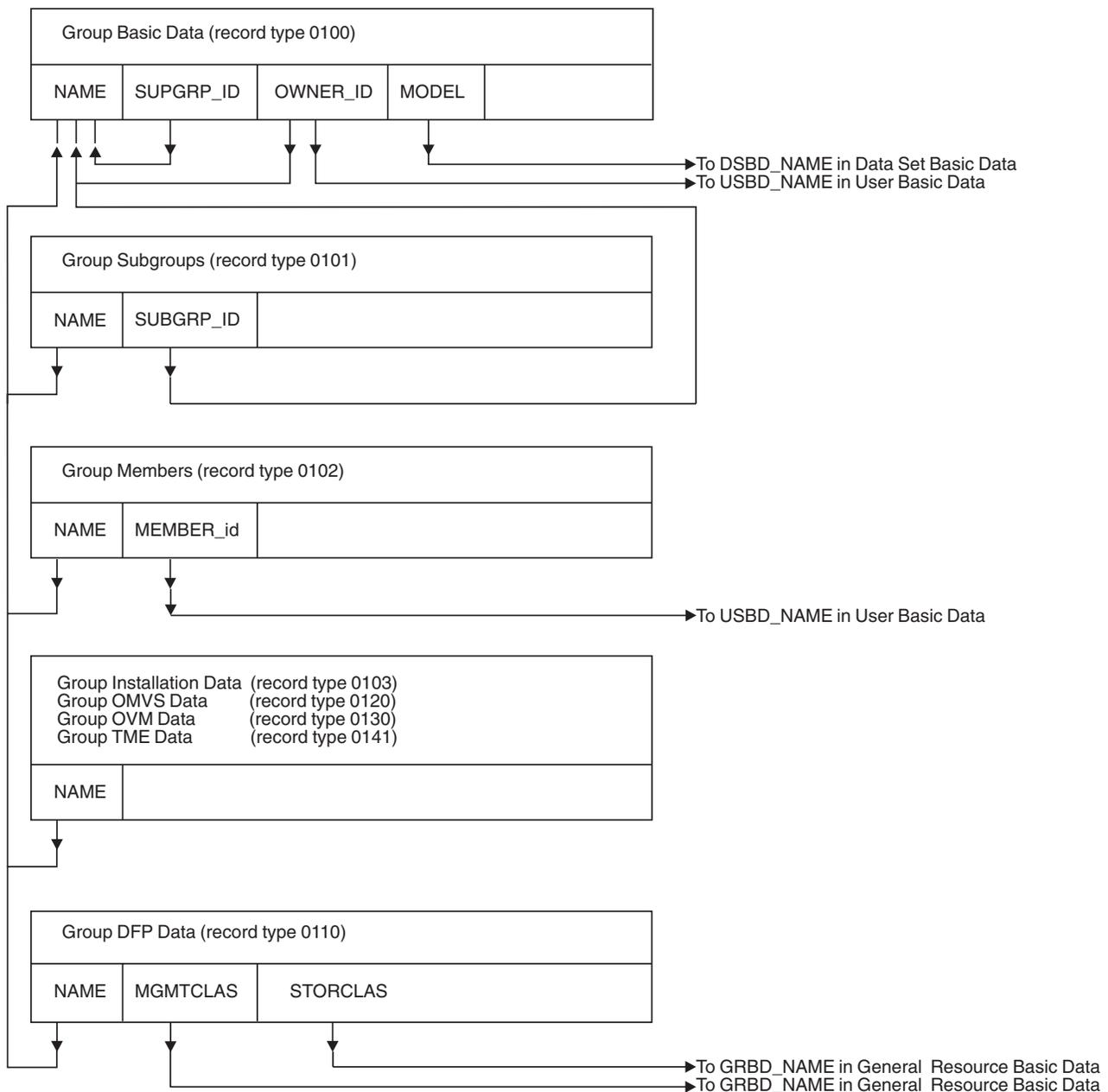


Figure 1. Relationship among the Group Record Types

User Records

The high level qualifier which represents the table identifier is omitted. For user records, these qualifiers are:

Record Name	Record Type	Record Prefix
User Basic Data	0200	USBD
User Categories	0201	USCAT
User Classes	0202	USCLA
User Group Connections	0203	USGCON
User Installation Data	0204	USINSTD
User Connect Data	0205	USCON
User RRSF Data	0206	USRSF
User Certificate Data	0207	USCERT
User Mappings Record	0208	USNMAP
User DFP Data	0210	USDFP

User TSO Data	0220	USTSO
User CICS Data	0230	USCICS
User CICS Operator Classes	0231	USCOPC
User Language Data	0240	USLAN
User OPERPARM Data	0250	USOPR
User OPERPARM Scope	0251	USOPRP
User WORKATTR Data	0260	USWRK
User OMVS Data	0270	USOMVS
User NETVIEW Segment	0280	USNETV
User OPCLASS	0281	USNOPC
User DOMAINS	0282	USNDOM
User DCE Data	0290	USDCE
User OVM Data	02A0	USOVM
User LNOTES Data	02B0	USLNOT
User NDS Data	02C0	USNDS
User KERB Data	02D0	USKERB
User PROXY Data	02E0	USPROXY
User EIM Data	02F0	USEIM

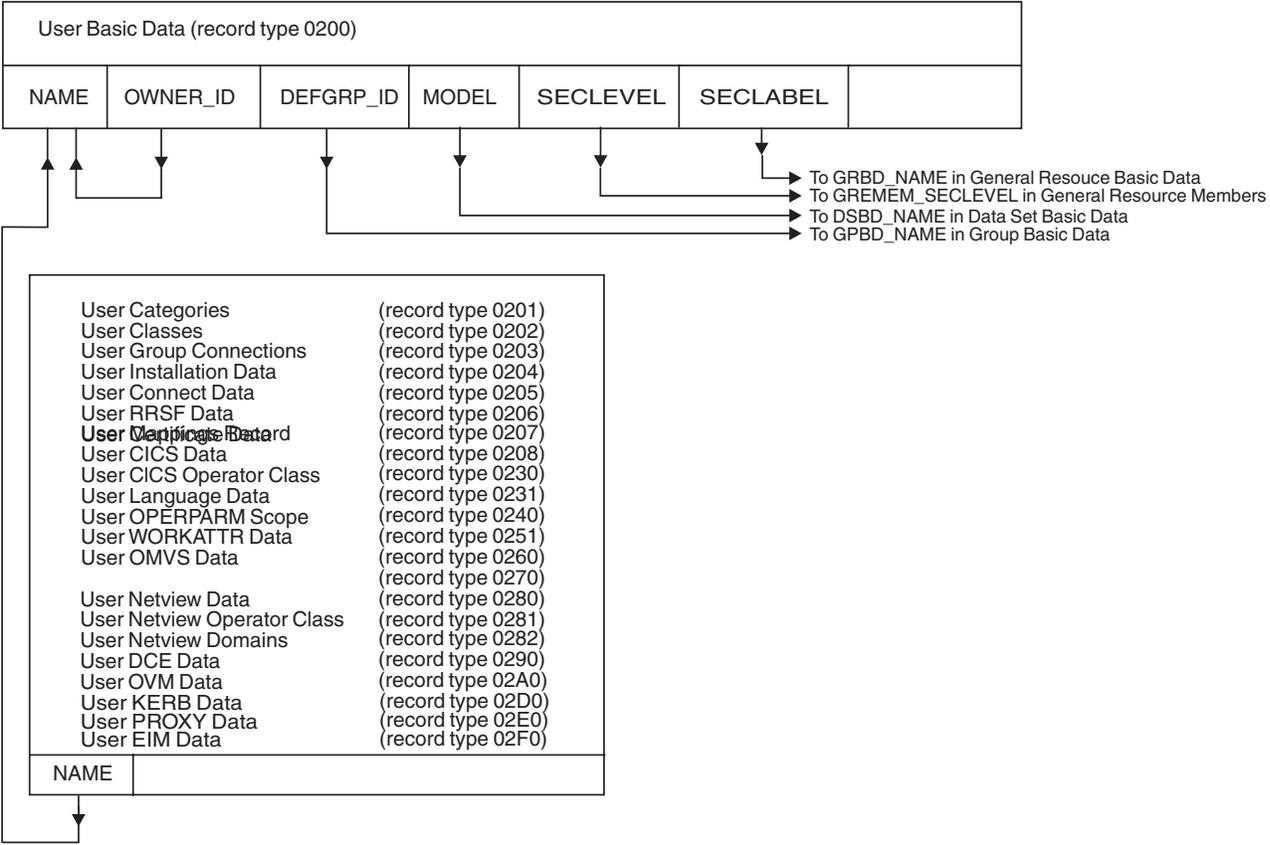


Figure 2. Relationship among the User Record Types (Part 1 of 2)

Database Unload—IRRDBU00

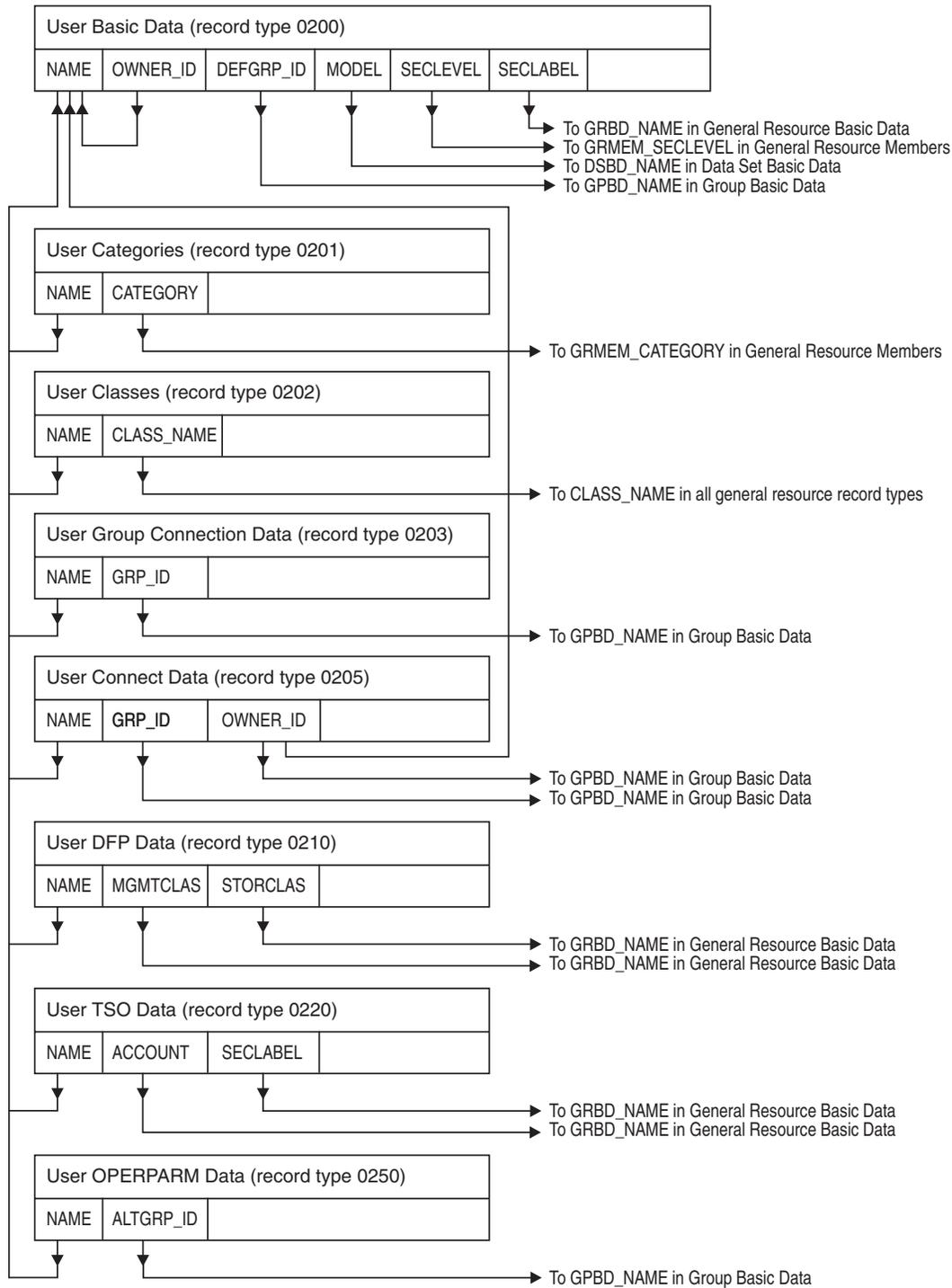


Figure 3. Relationship among the User Record Types (Part 2 of 2)

Data Set Records

The high level qualifier which represents the table identifier is omitted. For data set records, these qualifiers are:

Record Name	Record Type	Record Prefix
Data Set Basic Data	0400	DSBD
Data Set Categories	0401	DSCAT
Data Set Conditional Access	0402	DSCACC

Data Set Volumes	0403	DSVOL
Data Set Access	0404	DSACC
Data Set Installation Data	0405	DSINSTD
Data Set DFP Data	0410	DSDFP
Data Set TME Role Record	0421	DSTME

The NAME/VOL field is a concatenation of the NAME field and VOLUME field.

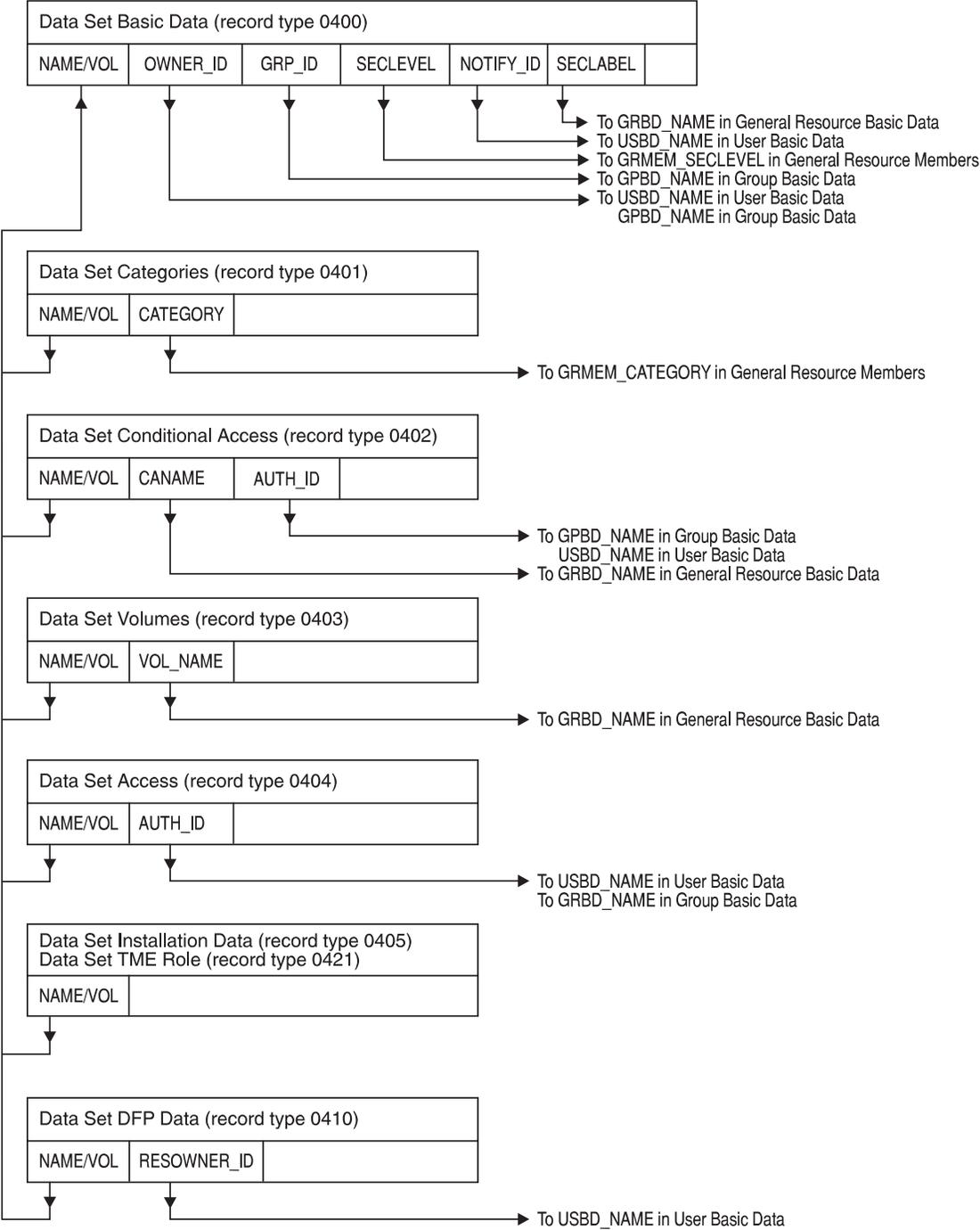


Figure 4. Relationship among the Data Set Record Types

General Resource Records

Database Unload—IRRDBU00

The high level qualifier which represents the table identifier is omitted. For general resource records, these qualifiers are:

Record Name	Record Type	Record Prefix
General Resource Basic Data	0500	GRBD
General Resource Tape Volume Data	0501	GRTVOL
General Resource Categories	0502	GRCAT
General Resource Members	0503	GRMEM
General Resource Volumes	0504	GRVOL
General Resource Access	0505	GRACC
General Resource Installation Data	0506	GRINSTD
General Resource Conditional Access	0507	GRCACC
General Filter Data Record	0508	GRFLTR
General Resource Session Data	0510	GRSES
General Resource Session Entities	0511	GRSESE
General Resource DLF Data	0520	GRDLF
General Resource DLF Job Names	0521	GRDLFJ
General Resource Started Task Data	0540	GRST
General Resource SystemView Data	0550	GRSV
General Resource Certificate Data	0560	GRCERT
General Resource Certificate Record	0561	CERTR
General Resource Key Ring Data	0562	KEYR
General Resource TME Data Record	0570	GRTME
General Resource TME Child Record	0571	GRTMEC
General Resource TME Resource Record	0572	GRTMER
General Resource TME Group Record	0573	GRTMEG
General Resource TME Role Record	0574	GRTMEE
General Resource KERB Data	0580	GRKERB
General Resource PROXY Data	0590	GRPROXY
General Resource EIM Data	05A0	GREIM

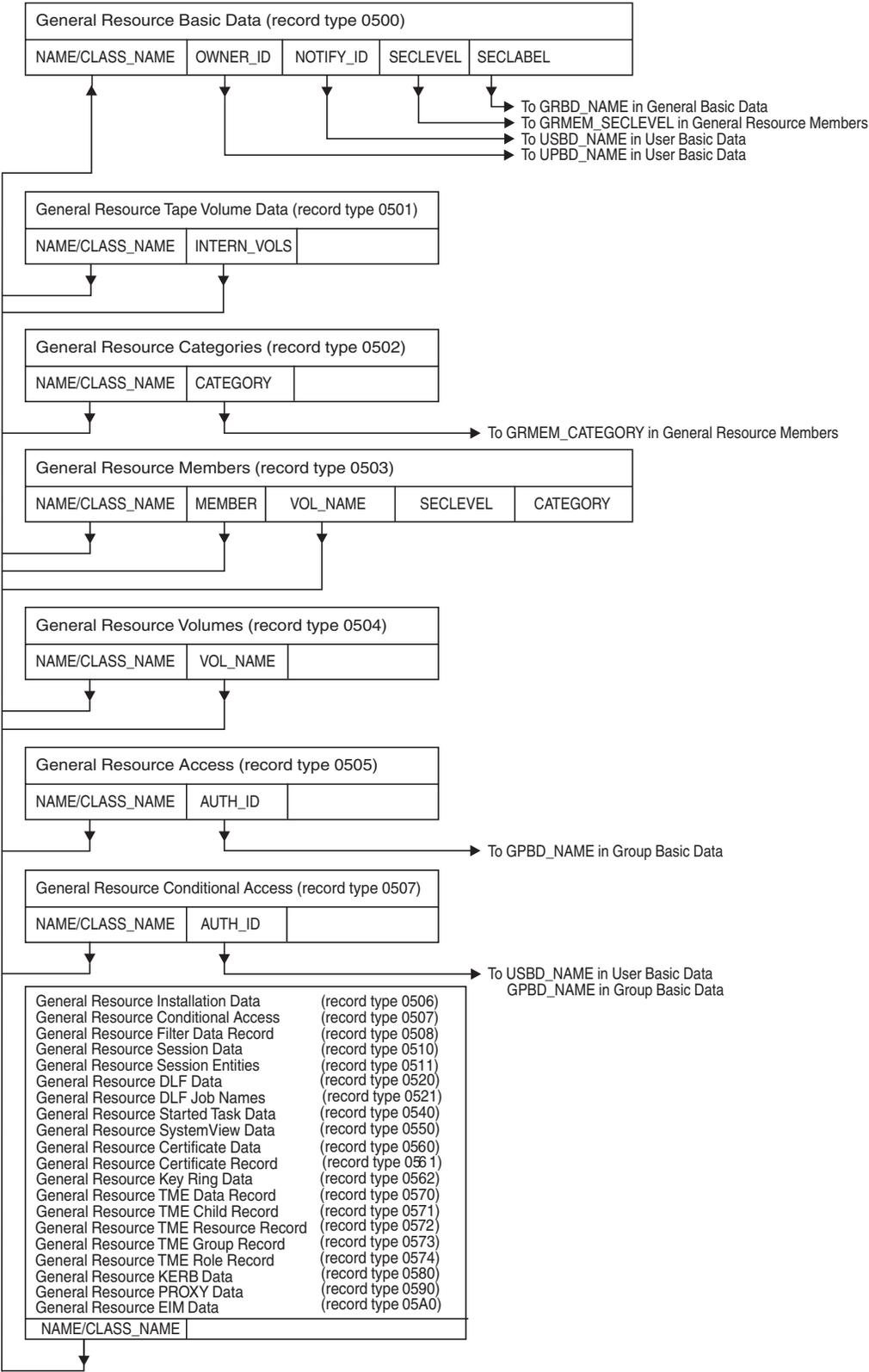


Figure 5. Relationship among the General Resource Record Types

Conversion Rules of the Database Unload Utility

In unloading the database, these rules were followed:

- Each repeat group has its own record type
For example, the repeat group representing the access list for data sets covered by a profile is ACL2CNT (the field name in the template). There is a data set access record (type 0404) created for each entry in the access list.
- Flag fields that are not mutually exclusive values (for example, 8-bit flags where more than one bit could be on at once) are defined as separate fields.
When this field is processed, it is unloaded as a 4-character field, with the values YES and NO as valid values. The field is left-justified.
- Flag fields that have mutually exclusive settings are unloaded as 8-character fields with a value corresponding to each bit setting.
For example, the UACC in a data set profile is a flag field in which each bit position corresponds to a universal access. The utility translates this single flag field into an 8-byte string with the value NONE, READ, UPDATE, CONTROL, or ALTER. If the flag field contains a value which is undefined, then the utility unloads the value as X<cc>, where cc is the hexadecimal value of the flag field.
- Encrypted and reserved fields are not unloaded.
- A maximum of 255 bytes are unloaded for any field, with the exception of the HOME_PATH and PROGRAM fields in a user's OMVS segment, HOME_PATH, PROGRAM, and FSROOT fields in a user's OVM segment and the DCE_NAME and HOMECCELL fields in a user's DCE segment for which 1023 bytes are unloaded.
- Fields for the installation's data, such as INSTDATA or the USRxx fields, are unloaded without any decoding. The USRFLG field, however, is treated as a hexadecimal value and is represented by X<cc>.
- A single byte with the value blank (X'40') is placed between each field in the output record. This makes it easier to understand the output file when it is viewed.
- Fields in the database which contain null data have blanks unloaded, with the exception of integer fields, which have a zero value unloaded. (Data is treated as null if 'FF' is coded as the default value for a character set in the base segment or if zeros are used in the character field in any segment other than the base segment.)

Record Formats Produced by the Database Unload Utility

The following sections contain a detailed description of the records that are produced by the database unload utility.

Each row in the tabular description of the records that are produced by the utility contains five pieces of information:

1. Descriptive name for the field
2. Type of field

Char	Character data.
Int	Integer–EBCDIC numeric data.
Time	A time value, in the form hh:mm:ss.
Date	A date value, in the form yyyy-mm-dd.
Yes/No	Flag data, having the value YES or NO.
3. Starting position for the field
4. Ending position for the field
5. Free form description of the field, which may contain the valid value constraints.

The complete record formats are located as follows:

- Group records, see “Group Record Formats”
- User records, see “User Record Formats” on page 261
- Data Set records, see “Data Set Record Formats” on page 275
- General Resource records, see “General Resource Record Formats” on page 279

Note: For some applications, such as SQL/DS, the start and end positions must account for a 4-position length indicator at the front of each record. For applications such as these, 4 would be added to each of the start and end positions indicated.

Group Record Formats

The records associated with groups are:

- Group Basic Data
- Group Subgroups
- Group Members
- Group Installation Data
- Group DFP Data
- Group OMVS Data
- Group OVM Data
- Group TME Role Record

Group Basic Data Record (0100): The Group Basic Data record defines the basic information that defines a group. There is one record per group.

Table 158. Group Basic Data Record. Defines the basic information about a group.

Field Name	Type	Position		Comments
		Start	End	
GPBD_RECORD_TYPE	Int	1	4	Record type of the Group Basic Data record (0100).
GPBD_NAME	Char	6	13	Group name as taken from the profile name.
GPBD_SUPGRP_ID	Char	15	22	Name of the superior group to this group.
GPBD_CREATE_DATE	Date	24	33	Date that the group was defined.
GPBD_OWNER_ID	Char	35	42	The user ID or group name which owns the profile.
GPBD_UACC	Char	44	51	The default universal access. Valid values are NONE for all groups other than the VSAMDSET group which has CREATE.
GPBD_NOTERMUACC	Yes/No	53	56	Indicates if the group must be specifically authorized to use a particular terminal through the use of the PERMIT command.
GPBD_INSTALL_DATA	Char	58	312	Installation-defined data.
GPBD_MODEL	Char	314	357	Data set profile that is used as a model for this group.
GPBD_UNIVERSAL	Yes/No	359	362	Indicates if the group has the UNIVERSAL attribute.

Group Subgroups Record (0101): The Group Subgroups record defines the relationship between a group and any subgroups that are within the group. There is one record per group/subgroup combination.

Table 159. Group Subgroups Record. Defines the relationship between a group and a subgroup.

Field Name	Type	Position		Comments
		Start	End	
GPSGRP_RECORD_TYPE	Int	1	4	Record type of the Group Subgroups record (0101).
GPSGRP_NAME	Char	6	13	Group name as taken from the profile name.
GPSGRP_SUBGRP_ID	Char	15	22	The name of a subgroup within the group.

Database Unload—IRRDBU00

Group Members Record (0102): The Group Members record defines the relationship between a group and the members of the group. There is one record per group/member combination.

Table 160. Group Members Record. Defines the relationship between a group and a member of the group.

Field Name	Type	Position		Comments
		Start	End	
GPMEM_RECORD_TYPE	Int	1	4	Record type of the Group Members record (0102).
GPMEM_NAME	Char	6	13	Group name as taken from the profile name.
GPMEM_MEMBER_ID	Char	15	22	A user ID within the group.
GPMEM_AUTH	Char	24	31	Indicates the authority that the user ID has within the group. Valid values are USE, CONNECT, JOIN, and CREATE.

Group Installation Data Record (0103): The Group Installation Data record defines the user data associated with a group.

This record type contains the data stored in the USRCNT repeat group, which is a field in the RACF database that is reserved for your installation's use. None of the RACF commands manipulate this field. Do not confuse this field with the GPBD_INSTALL_DATA field, shown in Table 160, which you enter into the database using the ADDGROUP and ALTGROUP commands.

There is one record per group/installation data combination.

Table 161. Group Installation Data Record. Defines the user-specified information associated with a group.

Field Name	Type	Position		Comments
		Start	End	
GPINSTD_RECORD_TYPE	Int	1	4	Record type of the Group Installation Data record (0103).
GPINSTD_NAME	Char	6	13	Group name as taken from the profile name.
GPINSTD_USR_NAME	Char	15	22	The name of the installation-defined field.
GPINSTD_USR_DATA	Char	24	278	The data for the installation-defined field.
GPINSTD_USR_FLAG	Char	280	287	The flag for the installation-defined field in the form X<cc>.

Group DFP Data Record (0110): The Group DFP Data record defines the information required by the System Managed Storage (SMS) facility of the Data Facility Product (DFP). The fields in these records define the characteristics of the data that this profile protects.

There is one record per group/DFP data combination.

Table 162. Group DFP Data Record. Defines the default System Managed Storage values for a group.

Field Name	Type	Position		Comments
		Start	End	
GPDFP_RECORD_TYPE	Int	1	4	Record type of the Group DFP Data record (0110).
GPDFP_NAME	Char	6	13	Group name as taken from the profile name.
GPDFP_DATAAPPL	Char	15	22	Default application name for the group.
GPDFP_DATACLAS	Char	24	31	Default data class for the group.
GPDFP_MGMTCLAS	Char	33	40	Default management class for the group.
GPDFP_STORCLAS	Char	42	49	Default storage class for the group.

Group OMVS Data Record (0120):

The Group OMVS Data record defines the information required by z/OS UNIX to verify that users are associated with a valid z/OS UNIX group identifier (GID). These records define the GIDs that have been assigned to RACF groups.

There is one record per group/GID combination.

Table 163. Group OMVS Data Record. Defines the z/OS UNIX group identifier (GID) for a RACF group.

Field Name	Type	Position		Comments
		Start	End	
GPOMVS_RECORD_TYPE	Int	1	4	Record type of the Group OMVS Data record (0120).
GPOMVS_NAME	Char	6	13	Group name as taken from the profile name.
GPOMVS_GID	Char	15	24	OMVS z/OS UNIX group identifier (GID) associated with the group name from the profile.

Group OVM Data Record (0130): The Group OVM Data record defines the z/OS UNIX VM group identifiers (GIDs) that have been assigned to RACF groups.

There is one record per group/GID combination.

Table 164. Group OVM Data Record. Defines the z/OS UNIX group identifier (GID) for a RACF group.

Field Name	Type	Position		Comments
		Start	End	
GPOVM_RECORD_TYPE	Int	1	4	Record type of the Group OVM Data record (0130).
GPOVM_NAME	Char	6	13	Group name as taken from the profile name.
GPOVM_GID	Char	15	24	OVM z/OS UNIX group identifier (GID) associated with the group name from the profile.

Group TME Role Record (0141): The Group TME Data record identifies ROLE profiles in which the group is referenced.

There is one record per group/role combination.

Table 165. Group TME Data Record

Field Name	Type	Position		Comments
		Start	End	
GPTME_RECORD_TYPE	Int	1	4	Record type of the Group TME Data record (0141).
GPTME_NAME	Char	6	13	Group name as taken from the profile name.
GPTME_ROLE	Char	15	260	Role profile name.

User Record Formats

The records associated with users are:

- User Basic Data
- User Categories
- User Classes
- User Group Connections
- User Installation Data
- User Connect Data
- User RRSF Data
- User Certificate Name
- User Mappings Record
- User DFP Data
- User TSO Data
- User CICS Data

Database Unload—IRRDBU00

- User CICS Operator Classes
- User Language Data
- User OPERPARM Data
- User OPERPARM Scope
- User WORKATTR Data
- User OMVS Data
- User NETVIEW Segment
- User OPCLASS
- User DOMAINS
- User DCE Data
- User OVM Data
- User LNOTES Data
- User NDS Data
- User KERB Data
- User PROXY Data
- User EIM Data

User Basic Data Record (0200): The User Basic Data record defines the basic information about a user. There is one record per user.

Table 166. User Basic Data Record. Defines the basic information about a user.

Field Name	Type	Position		Comments
		Start	End	
USBD_RECORD_TYPE	Int	1	4	Record type of the User Basic Data record (0200).
USBD_NAME	Char	6	13	User ID as taken from the profile name.
USBD_CREATE_DATE	Date	15	24	The date that the profile was created.
USBD_OWNER_ID	Char	26	33	The user ID or group name which owns the profile.
USBD_ADSP	Yes/No	35	38	Does the user have the ADSP attribute?
USBD_SPECIAL	Yes/No	40	43	Does the user have the SPECIAL attribute?
USBD_OPER	Yes/No	45	48	Does the user have the OPERATIONS attribute?
USBD_REVOKE	Yes/No	50	53	Is the user REVOKEd?
USBD_GRPACC	Yes/No	55	58	Does the user have the GRPACC attribute?
USBD_PWD_INTERVAL	Int	60	62	The number of days that the user's password may be used.
USBD_PWD_DATE	Date	64	73	The date that the password was last changed.
USBD_PROGRAMMER	Char	75	94	The name associated with the user ID.
USBD_DEFGRP_ID	Char	96	103	The default group associated with the user.
USBD_LASTJOB_TIME	Time	105	112	The time that the user last entered the system.
USBD_LASTJOB_DATE	Date	114	123	The date that the user last entered the system.
USBD_INSTALL_DATA	Char	125	379	Installation-defined data.
USBD_UAUDIT	Yes/No	381	384	Do all RACHECK and RACDEF SVCs cause logging?
USBD_AUDITOR	Yes/No	386	389	Does this user have the AUDITOR attribute?
USBD_NOPWD	Char	391	394	"YES" indicates that this user ID may logon without a password using OID card. "NO" indicates that this user must specify a password. "PRO" indicates a protected user ID. See also <i>z/OS Security Server RACF Security Administrator's Guide</i> .
USBD_OIDCARD	Yes/No	396	399	Does this user have OIDCARD data?
USBD_PWD_GEN	Int	401	403	The current password generation number.
USBD_REVOKE_CNT	Int	405	407	The number of unsuccessful logon attempts.
USBD_MODEL	Char	409	452	The data set model profile name.
USBD_SECLEVEL	Int	454	456	The user's security level.

Table 166. User Basic Data Record (continued). Defines the basic information about a user.

Field Name	Type	Position		Comments
		Start	End	
USBD_REVOKE_DATE	Date	458	467	The date that the user will be revoked.
USBD_RESUME_DATE	Date	469	478	The date that the user will be resumed.
USBD_ACCESS_SUN	Yes/No	480	483	Can the user access the system on Sunday?
USBD_ACCESS_MON	Yes/No	485	488	Can the user access the system on Monday?
USBD_ACCESS_TUE	Yes/No	490	493	Can the user access the system on Tuesday?
USBD_ACCESS_WED	Yes/No	495	498	Can the user access the system on Wednesday?
USBD_ACCESS_THU	Yes/No	500	503	Can the user access the system on Thursday?
USBD_ACCESS_FRI	Yes/No	505	508	Can the user access the system on Friday?
USBD_ACCESS_SAT	Yes/No	510	513	Can the user access the system on Saturday?
USBD_START_TIME	Time	515	522	After what time may the user logon?
USBD_END_TIME	Time	524	531	After what time may the user not logon?
USBD_SECLABEL	Char	533	540	The user's default security label.
USBD_ATTRIBS	Char	542	549	Other user attributes (RSTD for users with RESTRICTED attribute).

User Categories Record (0201): The User Categories record defines the categories to which the user has access. There is one record per user/category combination.

Table 167. User Categories Record. Defines the categories that users can access.

Field Name	Type	Position		Comments
		Start	End	
USCAT_RECORD_TYPE	Int	1	4	Record type of the User Categories record (0201).
USCAT_NAME	Char	6	13	User ID as taken from the profile name.
USCAT_CATEGORY	Int	15	19	Category to which the user has access.

User Classes Record (0202): The User Classes record defines the classes in which the user can create profiles. There is one record per user/class combination.

Table 168. User Classes Record. Defines the classes in which users can create profiles.

Field Name	Type	Position		Comments
		Start	End	
USCLA_RECORD_TYPE	Int	1	4	Record type of the User Classes record (0202).
USCLA_NAME	Char	6	13	User ID as taken from the profile name.
USCLA_CLASS	Char	15	22	A class in which the user is allowed to define profiles.

User Group Connections Record (0203): The User Group Connections record defines the groups with which the user is associated. There is one record per user connection.

Table 169. User Group Connections Record. Defines the groups with which a user is associated.

Field Name	Type	Position		Comments
		Start	End	
USGCON_RECORD_TYPE	Int	1	4	Record type of the User Group Connections record (0203).
USGCON_NAME	Char	6	13	User ID as taken from the profile name.
USGCON_GRP_ID	Char	15	22	The group with which the user is associated.

Database Unload—IRRDBU00

User Installation Data Record (0204): The User Installation Data record defines the user data associated with a user ID.

This record type contains the data stored in the USRCNT repeat group, which is a field in the RACF database that is reserved for your installation's use. None of the RACF commands manipulate this field. Do not confuse this field with the USER_INSTALL_DATA field, shown in Table 166 on page 262, which you enter into the database using the ADDUSER and ALTUSER commands.

Table 170. User Installation Data Record. Defines the user-specified information associated with a user ID.

Field Name	Type	Position		Comments
		Start	End	
USINSTD_RECORD_TYPE	Int	1	4	Record type of the User Installation Data record (0204).
USINSTD_NAME	Char	6	13	User ID as taken from the profile name.
USINSTD_USR_NAME	Char	15	22	The name of the installation-defined field.
USINSTD_USR_DATA	Char	24	278	The data for the installation-defined field.
USINSTD_USR_FLAG	Char	280	287	The flag for the installation-defined field in the form X<cc>.

User Connect Data Record (0205): The User Connect Data record defines the relationships between users and groups. There is one record per user connection.

Table 171. User Connect Data Record. Defines the relationship between a user and a group.

Field Name	Type	Position		Comments
		Start	End	
USCON_RECORD_TYPE	Int	1	4	Record type of the User Connect Data record (0205).
USCON_NAME	Char	6	13	User ID as taken from the profile name.
USCON_GRP_ID	Char	15	22	The group name.
USCON_CONNECT_DATE	Date	24	33	The date that the user was connected.
USCON_OWNER_ID	Char	35	42	The owner of the user-group connection.
USCON_LASTCON_TIME	Time	44	51	Time that the user last connected to this group.
USCON_LASTCON_DATE	Date	53	62	Date that the user last connected to this group.
USCON_UACC	Char	64	71	The default universal access. Valid values are NONE for all user IDs other than IBMUSER, which has READ to SYS1, SYSCTLG, and VSAMDSET.
USCON_INIT_CNT	Int	73	77	The number of RACINITs issued for this user/group combination.
USCON_GRP_ADSP	Yes/No	79	82	Does this user have the ADSP attribute in this group?
USCON_GRP_SPECIAL	Yes/No	84	87	Does this user have GROUP-SPECIAL in this group?
USCON_GRP_OPER	Yes/No	89	92	Does this user have GROUP-OPERATIONS in this group?
USCON_REVOKE	Yes/No	94	97	Is this user revoked?
USCON_GRP_ACC	Yes/No	99	102	Does this user have the GRPACC attribute?
USCON_NOTERMUACC	Yes/No	104	107	Does this user have the NOTERMUACC attribute in this group?
USCON_GRP_AUDIT	Yes/No	109	112	Does this user have the GROUP-AUDITOR attribute in this group?
USCON_REVOKE_DATE	Date	114	123	The date that the user's connection to the group will be revoked.
USCON_RESUME_DATE	Date	125	134	The date that the user's connection to the group will be resumed.

User RRSF Data Record (0206): The User RRSF Data record defines the information required by RRSF (RACF remote sharing facility). There is one record per user/RRSF data combination.

Table 172. User RRSF Data Record. Defines the RRSF fields unloaded.

Field Name	Type	Position		Comments
		Start	End	
USRSF_RECORD_TYPE	Int	1	4	Record type of the RRSF data record (0206).
USRSF_NAME	Char	6	13	User ID as taken from the profile name.
USRSF_TARG_NODE	Char	15	22	Target node name.
USRSF_TARG_USER_ID	Char	24	31	Target user ID.
USRSF_VERSION	Int	33	35	Version of this record.
USRSF_PEER	Yes/No	37	40	Is this a peer user ID?
USRSF_MANAGING	Yes/No	42	45	Is USRSF_NAME managing this ID?
USRSF_MANAGED	Yes/No	47	50	Is USRSF_NAME being managed by this ID?
USRSF_REMOTE_PEND	Yes/No	52	55	Is this remote RACF association pending?
USRSF_LOCAL_PEND	Yes/No	57	60	Is this local RACF association pending?
USRSF_PWD_SYNC	Yes/No	62	65	Is there password synchronization with this user ID?
USRSF_REM_REFUSAL	Yes/No	67	70	Was a system error encountered on the remote system?
USRSF_DEFINE_DATE	Date	72	81	GMT date stamp for when this record was defined.
USRSF_DEFINE_TIME	Time	83	97	GMT time stamp for when this record was defined.
USRSF_ACCEPT_DATE	Date	99	108	GMT date stamp when this association was approved or refused. Based on the REMOTE_REFUSAL bit setting.
USRSF_ACCEPT_TIME	Time	110	124	GMT time stamp when this association was approved or refused. Based on the REMOTE_REFUSAL bit setting.
USRSF_CREATOR_ID	Char	126	133	User ID who created this entry.

User Certificate Name Record (0207): The User Certificate Name record defines the names of the certificate profiles in the DIGTCERT class that are associated with this user ID.

Note: RACF does not unload all fields in profiles in the DIGTCERT class. The digital certificate itself is not readable text and is the only field in the CERTDATA segment. Therefore, RACF bypasses the unloading of the CERTDATA segment of general resource profiles.

Table 173. User Certificate Name Record. Defines the certificate profiles associated with this user ID.

Field Name	Type	Position		Comments
		Start	End	
USCERT_RECORD_TYPE	Int	1	4	Record type of the Certificate name record (0207).
USCERT_NAME	Char	6	13	User ID as taken from the profile name.
USCERT_CERT_NAME	Char	15	260	Digital Certificate name.
USCERT_CERTLABL	Char	262	293	Digital Certificate label.

User Associated Mappings Record (0208): The User Associated Mappings Record defines the certificate name filter in the DIGTNMAP class associated with this user ID.

Database Unload—IRRDBU00

Table 174. User Associated Mappings Record. Defines the mappings record associated with this user ID.

Field Name	Type	Position		Comments
		Start	End	
USNMAP_RECORD_TYPE	Int	1	4	Record type of the User Associated Mappings record (0208).
USNMAP_NAME	Char	6	13	User ID as taken from the profile name.
USNMAP_LABEL	Char	15	46	The label associated with this mapping.
USNMAP_MAP_NAME	Char	48	293	The name of the DIGTNMAP profile associated with this user.

User DFP Data Record (0210): The User DFP Data record defines the information required by the System Managed Storage facility of the Data Facility Product (DFP). The fields in these records define the characteristics of the data that are created by the user. There is one record per user/DFP data combination.

Table 175. User DFP Data Record. Defines the default System Managed Storage values for a user.

Field Name	Type	Position		Comments
		Start	End	
USDFP_RECORD_TYPE	Int	1	4	Record type of the User DFP data record (0210).
USDFP_NAME	Char	6	13	User ID as taken from the profile name.
USDFP_DATAAPPL	Char	15	22	Default application name for the user.
USDFP_DATACLAS	Char	24	31	Default data class for the user.
USDFP_MGMTCLAS	Char	33	40	Default management class for the user.
USDFP_STORCLAS	Char	42	49	Default storage class for the user.

User TSO Data Record (0220): The User TSO Data record defines the information required by TSO/E. There is one record per TSO user.

Table 176. User TSO Data Record. Defines the TSO information about a user.

Field Name	Type	Position		Comments
		Start	End	
USTSO_RECORD_TYPE	Int	1	4	Record type of the User TSO Data record (0220).
USTSO_NAME	Char	6	13	User ID as taken from the profile name.
USTSO_ACCOUNT	Char	15	54	The default account number.
USTSO_COMMAND	Char	56	135	The command issued at LOGON.
USTSO_DEST	Char	137	144	The default destination identifier.
USTSO_HOLD_CLASS	Char	146	146	The default hold class.
USTSO_JOB_CLASS	Char	148	148	The default job class.
USTSO_LOGON_PROC	Char	150	157	The default logon procedure.
USTSO_LOGON_SIZE	Int	159	168	The default logon region size.
USTSO_MSG_CLASS	Char	170	170	The default message class.
USTSO_LOGON_MAX	Int	172	181	The maximum logon region size.
USTSO_PERF_GROUP	Int	183	192	The performance group associated with the user.
USTSO_SYSOUT_CLASS	Char	194	194	The default sysout class.
USTSO_USER_DATA	Char	196	203	The TSO user data, in hexadecimal in the form X<cccc>.
USTSO_UNIT_NAME	Char	205	212	The default SYSDA device.
USTSO_SECLABEL	Char	214	221	The default logon security label.

User CICS Data Record (0230): The User CICS Data record defines the data required by the Customer Information Control System (CICS). There is one record per user/CICS data combination.

Table 177. User CICS Data Record. Defines the CICS information about a user.

Field Name	Type	Position		Comments
		Start	End	
USCICS_RECORD_TYPE	Int	1	4	Record type of the User CICS Data record (0230).
USCICS_NAME	Char	6	13	User ID as taken from the profile name.
USCICS_OPIDENT	Char	15	17	The CICS operator identifier.
USCICS_OPPRTY	Int	19	23	The CICS operator priority.
USCICS_NOFORCE	Yes/No	25	28	Is the extended recovery facility (XRF) NOFORCE option in effect?
USCICS_TIMEOUT	Char	30	34	The terminal time-out value. Expressed in hh:mm

User CICS Operator Classes Record (0231): The User CICS Operator Classes record defines the classes associated with a CICS operator. There is one record per user/CICS operator class combination.

Table 178. User CICS Operator Class Record. Defines the classes associated with a CICS operator.

Field Name	Type	Position		Comments
		Start	End	
USCOPC_RECORD_TYPE	Int	1	4	Record type of the User CICS Operator Class record (0231).
USCOPC_NAME	Char	6	13	User ID as taken from the profile name.
USCOPC_OPCLASS	Char	15	17	The class associated with the CICS operator.

User Language Data Record (0240): The User Language Data record defines the primary and default languages for the user. There is one record per user/language combination.

Table 179. User Language Data Record. Defines the primary and secondary languages for the user.

Field Name	Type	Position		Comments
		Start	End	
USLAN_RECORD_TYPE	Int	1	4	Record type of the User Language Data record (0240).
USLAN_NAME	Char	6	13	User ID as taken from the profile name.
USLAN_PRIMARY	Char	15	17	The primary language for the user.
USLAN_SECONDARY	Char	19	21	The secondary language for the user.

User OPERPARM Data Record (0250): The User OPERPARM Data record defines the operator characteristics for the user. There is one record per user/OPERPARM data combination.

Table 180. User OPERPARM Data Record. Defines the operator definition information for a console operator.

Field Name	Type	Position		Comments
		Start	End	
USOPR_RECORD_TYPE	Int	1	4	Record type of the User OPERPARM Data record (0250).
USOPR_NAME	Char	6	13	User ID as taken from the profile name.
USOPR_STORAGE	Int	15	19	The number of megabytes of storage that can be used for message queuing.
USOPR_MASTERAUTH	Yes/No	21	24	Does this user have MASTER console authority?

Database Unload—IRRDBU00

Table 180. User OPERPARM Data Record (continued). Defines the operator definition information for a console operator.

Field Name	Type	Position		Comments
		Start	End	
USOPR_ALLAUTH	Yes/No	26	29	Does this user have ALL console authority?
USOPR_SYSAUTH	Yes/No	31	34	Does this user have SYSAUTH console authority?
USOPR_IOAUTH	Yes/No	36	39	Does this user have I/O console authority?
USOPR_CONSAUTH	Yes/No	41	44	Does this user have CONS console authority?
USOPR_INFOAUTH	Yes/No	46	49	Does this user have INFO console authority?
USOPR_TIMESTAMP	Yes/No	51	54	Do console messages contain a timestamp?
USOPR_SYSTEMID	Yes/No	56	59	Do console messages contain a system ID?
USOPR_JOBID	Yes/No	61	64	Do console messages contain a job ID?
USOPR_MSGID	Yes/No	66	69	Do console messages contain a message ID?
USOPR_X	Yes/No	71	74	Are the job name and system name to be suppressed for messages issued from the JES3 global processor?
USOPR_WTOR	Yes/No	76	79	Does the console receive WTOR messages?
USOPR_IMMEDIATE	Yes/No	81	84	Does the console receive <i>immediate</i> messages?
USOPR_CRITICAL	Yes/No	86	89	Does the console receive <i>critical event</i> messages?
USOPR_EVENTUAL	Yes/No	91	94	Does the console receive <i>eventual event</i> messages?
USOPR_INFO	Yes/No	96	99	Does the console receive <i>informational</i> messages?
USOPR_NOBROADCAST	Yes/No	101	104	Are broadcast messages to this console suppressed?
USOPR_ALL	Yes/No	106	109	Does the console receive all messages?
USOPR_JOBNAME	Yes/No	111	114	Are job names monitored?
USOPR_JOBNAMEST	Yes/No	116	119	Are job names monitored with timestamps displayed?
USOPR_SESS	Yes/No	121	124	Are user IDs displayed with each TSO initiation and termination?
USOPR_SESST	Yes/No	126	129	Are user IDs and timestamps displayed with each TSO initiation and termination?
USOPR_STATUS	Yes/No	131	134	Are data set names and dispositions displayed with each data set that is freed?
USOPR_ROUTE001	Yes/No	136	139	Is this console enabled for route code 001?
USOPR_ROUTE002	Yes/No	141	144	Is this console enabled for route code 002?
USOPR_ROUTE003	Yes/No	146	149	Is this console enabled for route code 003?
USOPR_ROUTE004	Yes/No	151	154	Is this console enabled for route code 004?
USOPR_ROUTE005	Yes/No	156	159	Is this console enabled for route code 005?
USOPR_ROUTE006	Yes/No	161	164	Is this console enabled for route code 006?
USOPR_ROUTE007	Yes/No	166	169	Is this console enabled for route code 007?
USOPR_ROUTE008	Yes/No	171	174	Is this console enabled for route code 008?
USOPR_ROUTE009	Yes/No	176	179	Is this console enabled for route code 009?
USOPR_ROUTE010	Yes/No	181	184	Is this console enabled for route code 010?
USOPR_ROUTE011	Yes/No	186	189	Is this console enabled for route code 011?
USOPR_ROUTE012	Yes/No	191	194	Is this console enabled for route code 012?
USOPR_ROUTE013	Yes/No	196	199	Is this console enabled for route code 013?
USOPR_ROUTE014	Yes/No	201	204	Is this console enabled for route code 014?
USOPR_ROUTE015	Yes/No	206	209	Is this console enabled for route code 015?
USOPR_ROUTE016	Yes/No	211	214	Is this console enabled for route code 016?
USOPR_ROUTE017	Yes/No	216	219	Is this console enabled for route code 017?
USOPR_ROUTE018	Yes/No	221	224	Is this console enabled for route code 018?

Table 180. User OPERPARM Data Record (continued). Defines the operator definition information for a console operator.

Field Name	Type	Position		Comments
		Start	End	
USOPR_ROUTE019	Yes/No	226	229	Is this console enabled for route code 019?
USOPR_ROUTE020	Yes/No	231	234	Is this console enabled for route code 020?
USOPR_ROUTE021	Yes/No	236	239	Is this console enabled for route code 021?
USOPR_ROUTE022	Yes/No	241	244	Is this console enabled for route code 022?
USOPR_ROUTE023	Yes/No	246	249	Is this console enabled for route code 023?
USOPR_ROUTE024	Yes/No	251	254	Is this console enabled for route code 024?
USOPR_ROUTE025	Yes/No	256	259	Is this console enabled for route code 025?
USOPR_ROUTE026	Yes/No	261	264	Is this console enabled for route code 026?
USOPR_ROUTE027	Yes/No	266	269	Is this console enabled for route code 027?
USOPR_ROUTE028	Yes/No	271	274	Is this console enabled for route code 028?
USOPR_ROUTE029	Yes/No	276	279	Is this console enabled for route code 029?
USOPR_ROUTE030	Yes/No	281	284	Is this console enabled for route code 030?
USOPR_ROUTE031	Yes/No	286	289	Is this console enabled for route code 031?
USOPR_ROUTE032	Yes/No	291	294	Is this console enabled for route code 032?
USOPR_ROUTE033	Yes/No	296	299	Is this console enabled for route code 033?
USOPR_ROUTE034	Yes/No	301	304	Is this console enabled for route code 034?
USOPR_ROUTE035	Yes/No	306	309	Is this console enabled for route code 035?
USOPR_ROUTE036	Yes/No	311	314	Is this console enabled for route code 036?
USOPR_ROUTE037	Yes/No	316	319	Is this console enabled for route code 037?
USOPR_ROUTE038	Yes/No	321	324	Is this console enabled for route code 038?
USOPR_ROUTE039	Yes/No	326	329	Is this console enabled for route code 039?
USOPR_ROUTE040	Yes/No	331	334	Is this console enabled for route code 040?
USOPR_ROUTE041	Yes/No	336	339	Is this console enabled for route code 041?
USOPR_ROUTE042	Yes/No	341	344	Is this console enabled for route code 042?
USOPR_ROUTE043	Yes/No	346	349	Is this console enabled for route code 043?
USOPR_ROUTE044	Yes/No	351	354	Is this console enabled for route code 044?
USOPR_ROUTE045	Yes/No	356	359	Is this console enabled for route code 045?
USOPR_ROUTE046	Yes/No	361	364	Is this console enabled for route code 046?
USOPR_ROUTE047	Yes/No	366	369	Is this console enabled for route code 047?
USOPR_ROUTE048	Yes/No	371	374	Is this console enabled for route code 048?
USOPR_ROUTE049	Yes/No	376	379	Is this console enabled for route code 049?
USOPR_ROUTE050	Yes/No	381	384	Is this console enabled for route code 050?
USOPR_ROUTE051	Yes/No	386	389	Is this console enabled for route code 051?
USOPR_ROUTE052	Yes/No	391	394	Is this console enabled for route code 052?
USOPR_ROUTE053	Yes/No	396	399	Is this console enabled for route code 053?
USOPR_ROUTE054	Yes/No	401	404	Is this console enabled for route code 054?
USOPR_ROUTE055	Yes/No	406	409	Is this console enabled for route code 055?
USOPR_ROUTE056	Yes/No	411	414	Is this console enabled for route code 056?
USOPR_ROUTE057	Yes/No	416	419	Is this console enabled for route code 057?
USOPR_ROUTE058	Yes/No	421	424	Is this console enabled for route code 058?
USOPR_ROUTE059	Yes/No	426	429	Is this console enabled for route code 059?
USOPR_ROUTE060	Yes/No	431	434	Is this console enabled for route code 060?
USOPR_ROUTE061	Yes/No	436	439	Is this console enabled for route code 061?

Database Unload—IRRDBU00

Table 180. User OPERPARM Data Record (continued). Defines the operator definition information for a console operator.

Field Name	Type	Position		Comments
		Start	End	
USOPR_ROUTE062	Yes/No	441	444	Is this console enabled for route code 062?
USOPR_ROUTE063	Yes/No	446	449	Is this console enabled for route code 063?
USOPR_ROUTE064	Yes/No	451	454	Is this console enabled for route code 064?
USOPR_ROUTE065	Yes/No	456	459	Is this console enabled for route code 065?
USOPR_ROUTE066	Yes/No	461	464	Is this console enabled for route code 066?
USOPR_ROUTE067	Yes/No	466	469	Is this console enabled for route code 067?
USOPR_ROUTE068	Yes/No	471	474	Is this console enabled for route code 068?
USOPR_ROUTE069	Yes/No	476	479	Is this console enabled for route code 069?
USOPR_ROUTE070	Yes/No	481	484	Is this console enabled for route code 070?
USOPR_ROUTE071	Yes/No	486	489	Is this console enabled for route code 071?
USOPR_ROUTE072	Yes/No	491	494	Is this console enabled for route code 072?
USOPR_ROUTE073	Yes/No	496	499	Is this console enabled for route code 073?
USOPR_ROUTE074	Yes/No	501	504	Is this console enabled for route code 074?
USOPR_ROUTE075	Yes/No	506	509	Is this console enabled for route code 075?
USOPR_ROUTE076	Yes/No	511	514	Is this console enabled for route code 076?
USOPR_ROUTE077	Yes/No	516	519	Is this console enabled for route code 077?
USOPR_ROUTE078	Yes/No	521	524	Is this console enabled for route code 078?
USOPR_ROUTE079	Yes/No	526	529	Is this console enabled for route code 079?
USOPR_ROUTE080	Yes/No	531	534	Is this console enabled for route code 080?
USOPR_ROUTE081	Yes/No	536	539	Is this console enabled for route code 081?
USOPR_ROUTE082	Yes/No	541	544	Is this console enabled for route code 082?
USOPR_ROUTE083	Yes/No	546	549	Is this console enabled for route code 083?
USOPR_ROUTE084	Yes/No	551	554	Is this console enabled for route code 084?
USOPR_ROUTE085	Yes/No	556	559	Is this console enabled for route code 085?
USOPR_ROUTE086	Yes/No	561	564	Is this console enabled for route code 086?
USOPR_ROUTE087	Yes/No	566	569	Is this console enabled for route code 087?
USOPR_ROUTE088	Yes/No	571	574	Is this console enabled for route code 088?
USOPR_ROUTE089	Yes/No	576	579	Is this console enabled for route code 089?
USOPR_ROUTE090	Yes/No	581	584	Is this console enabled for route code 090?
USOPR_ROUTE091	Yes/No	586	589	Is this console enabled for route code 091?
USOPR_ROUTE092	Yes/No	591	594	Is this console enabled for route code 092?
USOPR_ROUTE093	Yes/No	596	599	Is this console enabled for route code 093?
USOPR_ROUTE094	Yes/No	601	604	Is this console enabled for route code 094?
USOPR_ROUTE095	Yes/No	606	609	Is this console enabled for route code 095?
USOPR_ROUTE096	Yes/No	611	614	Is this console enabled for route code 096?
USOPR_ROUTE097	Yes/No	616	619	Is this console enabled for route code 097?
USOPR_ROUTE098	Yes/No	621	624	Is this console enabled for route code 098?
USOPR_ROUTE099	Yes/No	626	629	Is this console enabled for route code 099?
USOPR_ROUTE100	Yes/No	631	634	Is this console enabled for route code 100?
USOPR_ROUTE101	Yes/No	636	639	Is this console enabled for route code 101?
USOPR_ROUTE102	Yes/No	641	644	Is this console enabled for route code 102?
USOPR_ROUTE103	Yes/No	646	649	Is this console enabled for route code 103?
USOPR_ROUTE104	Yes/No	651	654	Is this console enabled for route code 104?

Table 180. User OPERPARM Data Record (continued). Defines the operator definition information for a console operator.

Field Name	Type	Position		Comments
		Start	End	
USOPR_ROUTE105	Yes/No	656	659	Is this console enabled for route code 105?
USOPR_ROUTE106	Yes/No	661	664	Is this console enabled for route code 106?
USOPR_ROUTE107	Yes/No	666	669	Is this console enabled for route code 107?
USOPR_ROUTE108	Yes/No	671	674	Is this console enabled for route code 108?
USOPR_ROUTE109	Yes/No	676	679	Is this console enabled for route code 109?
USOPR_ROUTE110	Yes/No	681	684	Is this console enabled for route code 110?
USOPR_ROUTE111	Yes/No	686	689	Is this console enabled for route code 111?
USOPR_ROUTE112	Yes/No	691	694	Is this console enabled for route code 112?
USOPR_ROUTE113	Yes/No	696	699	Is this console enabled for route code 113?
USOPR_ROUTE114	Yes/No	701	704	Is this console enabled for route code 114?
USOPR_ROUTE115	Yes/No	706	709	Is this console enabled for route code 115?
USOPR_ROUTE116	Yes/No	711	714	Is this console enabled for route code 116?
USOPR_ROUTE117	Yes/No	716	719	Is this console enabled for route code 117?
USOPR_ROUTE118	Yes/No	721	724	Is this console enabled for route code 118?
USOPR_ROUTE119	Yes/No	726	729	Is this console enabled for route code 119?
USOPR_ROUTE120	Yes/No	731	734	Is this console enabled for route code 120?
USOPR_ROUTE121	Yes/No	736	739	Is this console enabled for route code 121?
USOPR_ROUTE122	Yes/No	741	744	Is this console enabled for route code 122?
USOPR_ROUTE123	Yes/No	746	749	Is this console enabled for route code 123?
USOPR_ROUTE124	Yes/No	751	754	Is this console enabled for route code 124?
USOPR_ROUTE125	Yes/No	756	759	Is this console enabled for route code 125?
USOPR_ROUTE126	Yes/No	761	764	Is this console enabled for route code 126?
USOPR_ROUTE127	Yes/No	766	769	Is this console enabled for route code 127?
USOPR_ROUTE128	Yes/No	771	774	Is this console enabled for route code 128?
USOPR_LOGCMDRESP	Char	776	783	Specifies the logging of command responses received by the extended operator. Valid values are SYSTEM, NO, and blank.
USOPR_MIGRATIONID	Yes/No	785	788	Is this extended operator to receive a migration ID?
USOPR_DELOPERMSG	Char	790	797	Does this extended operator receive delete operator messages? Valid values are NORMAL, ALL, and NONE.
USOPR_RETRIEVE_KEY	Char	799	806	Specifies a retrieval key used for searching. A null value is indicated by NONE.
USOPR_CMDSYS	Char	808	815	The name of the system that the extended operator is connected to for command processing.
USOPR_UD	Yes/No	817	820	Is this operator to receive undeliverable messages?
USOPR_ALTGRP_ID	Char	822	829	The default group associated with this operator.
USOPR_AUTO	Yes/No	831	834	Is this operator to receive messages automated within the sysplex?

User OPERPARM Scope (0251): The User OPERPARM Scope record defines the scope of the operator. There is one record per user/OPERPARM scope combination.

Database Unload—IRRDBU00

Table 181. User OPERPARM Scope Record. Defines the scope of an operator.

Field Name	Type	Position		Comments
		Start	End	
USOPRP_RECORD_TYPE	Int	1	4	Record type of the User OPERPARM Scope record (0251).
USOPRP_NAME	Char	6	13	User ID as taken from the profile name.
USOPRP_SYSTEM	Char	15	22	System name.

User WORKATTR Data Record (0260): The User WORKATTR Data record defines the logistical information for the user. There is one record per user/WORKATTR data combination.

Table 182. User WORKATTR Data Record. Defines the SYSOUT delivery information for a user.

Field Name	Type	Position		Comments
		Start	End	
USWRK_RECORD_TYPE	Int	1	4	Record type of the User WORKATTR Data record (0260).
USWRK_NAME	Char	6	13	User ID as taken from the profile name.
USWRK_AREA_NAME	Char	15	74	Area for delivery.
USWRK_BUILDING	Char	76	135	Building for delivery.
USWRK_DEPARTMENT	Char	137	196	Department for delivery.
USWRK_ROOM	Char	198	257	Room for delivery.
USWRK_ADDR_LINE1	Char	259	318	Address line 1.
USWRK_ADDR_LINE2	Char	320	379	Address line 2.
USWRK_ADDR_LINE3	Char	381	440	Address line 3.
USWRK_ADDR_LINE4	Char	442	501	Address line 4.
USWRK_ACCOUNT	Char	503	757	Account number.

User OMVS Data Record (0270): The User OMVS Data record defines the information required by z/OS UNIX to verify that users are associated with a valid z/OS UNIX user identifier (UID). These records define the UIDs which have been assigned to RACF users, their default directory, default program name, and user limits.

There is only one record per user/UID data combination.

Table 183. User OMVS Data Record. Defines the z/OS UNIX user identifier (UID) for a RACF user.

Field Name	Type	Position		Comments
		Start	End	
USOMVS_RECORD_TYPE	Int	1	4	Record type of the User OMVS Data record (0270).
USOMVS_NAME	Char	6	13	User name as taken from the profile name.
USOMVS_UID	Char	15	24	OMVS z/OS UNIX user identifier (UID) associated with the user name from the profile.
USOMVS_HOME_PATH	Char	26	1048	OMVS HOME PATH associated with the z/OS UNIX user identifier (UID).
USOMVS_PROGRAM	Char	1050	2072	OMVS Default Program associated with the z/OS UNIX user identifier (UID).
USOMVS_CPUTIMEMAX	Int	2074	2083	OMVS maximum CPU time associated with the UID.
USOMVS_ASSIZEMAX	Int	2085	2094	OMVS maximum address space size associated with the UID.
USOMVS_FILEPROCMAX	Int	2096	2105	OMVS maximum active or open files associated with the UID.

Table 183. User OMVS Data Record (continued). Defines the z/OS UNIX user identifier (UID) for a RACF user.

Field Name	Type	Position		Comments
		Start	End	
USOMVS_PROCUSERMAX	Int	2107	2116	OMVS maximum number of processes associated with the UID.
USOMVS_THREADSMAX	Int	2118	2127	OMVS maximum number of threads associated with the UID.
USOMVS_MMAPAREAMAX	Int	2129	2138	OMVS maximum mappable storage amount associated with the UID.

User NETVIEW Segment Record (0280): The User NETVIEW segment record defines the information required by NetView.

There is only one record per user profile that contains a NETVIEW segment.

Table 184. User NETVIEW Segment Record. Defines the NetView segment for a RACF user.

Field Name	Type	Position		Comments
		Start	End	
USNETV_RECORD_TYPE	Int	1	4	Record type of the user NETVIEW segment record (0280).
USNETV_NAME	Char	6	13	User ID as taken from profile name
USNETV_IC	Char	15	269	Command list processed at logon
USNETV_CONSNAME	Char	271	278	Default console name
USNETV_CTL	Char	280	287	CTL value: GENERAL, GLOBAL, or SPECIFIC
USNETV_MSGRECVR	Yes/No	289	292	Eligible to receive unsolicited messages?
USNETV_NGMFADMN	Yes/No	294	297	Authorized to NetView graphic monitoring facility?
USNETV_NGMFVSPN	Char	299	306	Value of view span options

User OPCLASS Record (0281): The User OPCLASS record defines the information required by NetView.

There is only one record per OPCLASS specified in the NETVIEW segment.

Table 185. User OPCLASS Record. Defines the OPCLASS for a RACF user.

Field Name	Type	Position		Comments
		Start	End	
USNOPC_RECORD_TYPE	Int	1	4	Record type of the user OPCLASS record (0281).
USNOPC_NAME	Char	6	13	User ID as taken from the profile name
USNOPC_OPCLASS	Int	15	19	OPCLASS value from 1 to 2040

User DOMAINS Record (0282): The User DOMAINS record defines the information required by NetView.

There is only one record per DOMAIN specified in the NETVIEW segment.

Table 186. User DOMAINS Record. Defines the DOMAIN for a RACF user.

Field Name	Type	Position		Comments
		Start	End	
USNDOM_RECORD_TYPE	Int	1	4	Record type of the user DOMAINS record (0282).
USNDOM_NAME	Char	6	13	User ID as taken from the profile name
USNDOM_DOMAINS	Char	15	19	DOMAIN value.

User DCE Data Record (0290): The User DCE Data record defines the non-repeating group information that is contained within the user’s DCE segment.

Table 187. User DCE Data Record. Defines the non-repeating information in the user’s DCE segment.

Field Name	Type	Position		Comments
		Start	End	
USDCE_RECORD_TYPE	Int	1	4	Record type of the user DCE data record (0290).
USDCE_NAME	Char	6	13	RACF user name as taken from the profile name.
USDCE_UUID	Char	15	50	DCE UUID associated with the user name from the profile.
USDCE_DCE_NAME	Char	52	1074	DCE principal name associated with this user.
USDCE_HOMECELL	Char	1076	2098	Home cell name.
USDCE_HOMEUUID	Char	2100	2135	Home cell UUID.
USDCE_AUTOLOGIN	Yes/No	2137	2140	Is this user eligible for an automatic DCE login?

User OVM Data Record (02A0): The User OVM Data record defines the information required by OpenEdition VM. These records define the user identifiers (UIDs) which have been assigned to RACF users, their default directory, default program name, and the file system root.

Table 188. User OVM Data Record. Defines the UID for a RACF user.

Field Name	Type	Position		Comments
		Start	End	
USOVM_RECORD_TYPE	Int	1	4	Record type of the user OVM data record (02A0).
USOVM_NAME	Char	6	13	User name as taken from the profile name.
USOVM_UID	Char	15	24	OVM user identifier (UID) associated with the user name from the profile.
USOVM_HOME_PATH	Char	26	1048	OVM home path associated with the user identifier (UID).
USOVM_PROGRAM	Char	1050	2072	OVM default program associated with the user identifier (UID).
USOVM_FSROOT	Char	2074	3096	OVM file system root for this user.

User LNOTES Data Record (02B0): The User LNOTES Data record contains the Lotus Notes for z/OS information defined in the LNOTES segment of the user’s profile.

Table 189. User LNOTES Data Record. Defines the Lotus Notes information for the user.

Field Name	Type	Position		Comments
		Start	End	
USLNOT_RECORD_TYPE	Int	1	4	Record type of the LNOTES data record (02B0).
USLNOT_NAME	Char	6	13	User ID as taken from the profile name.
USLNOT_SNAME	Char	15	78	LNOTES short name associated with the user ID.

User NDS Data Record (02C0): The User NDS Data record contains the Novell Directory Services for OS/390 information defined in the NDS segment of the user’s profile.

Table 190. User NDS Data Record. Defines the NDS information for the user profile.

Field Name	Type	Position		Comments
		Start	End	
USNDS_RECORD_TYPE	Int	1	4	Record type of the NDS data record (02C0).
USNDS_NAME	Char	6	13	User ID as taken from the profile name.
USNDS_UNAME	Char	15	260	NDS user name associated with the user ID.

User KERB Data Record (02D0): The User KERB Data record defines the Kerberos principal information for a user. There is one record per user profile that contains a KERB segment.

Table 191. User KERB Data Record. Defines the KERB information for the user profile.

Field Name	Type	Position		Comments
		Start	End	
USKERB_RECORD_TYPE	Int	1	4	Record type of the User KERB segment record (02D0).
USKERB_NAME	Char	6	13	RACF user name as taken from the profile.
USKERB_KERBNAME	Char	15	254	The Kerberos principal name.
USKERB_MAX_LIFE	Int	256	265	Maximum ticket life.
USKERB_KEY_VERS	Int	267	269	Current key version.
USKERB_ENCRYPT_DES	Yes/No	271	274	Key encryption using DES is enabled.
USKERB_ENCRYPT_DES3	Yes/No	276	279	Key encryption using DES3 is enabled.
USKERB_ENCRYPT_DESD	Yes/No	281	284	Key encryption using DES with derivation is enabled.

User PROXY Record (02E0): The user PROXY record identifies default information related to the LDAP proxy for a user. There is only one record per user profile that contains a PROXY segment.

Table 192. User PROXY Record

Field Name	Type	Position		Comments
		Start	End	
USPROXY_RECORD_TYPE	Int	1	4	Record type of the user PROXY record (0590).
USPROXY_NAME	Char	6	13	RACF user name as taken from the profile name.
USPROXY_LDAP_HOST	Char	15	1037	LDAP server URL.
USPROXY_BIND_DN	Char	1039	2061	LDAP BIND distinguished name.

User EIM Data Record (02F0): The user EIM record defines the LDAPBIND profile for a user. There is one record per user profile that contains the EIM segment.

Table 193. User EIM Record

Field Name	Type	Position		Comments
		Start	End	
USEIM_RECORD_TYPE	Int	1	4	Record type of the user EIM segment record (02F0).
USEIM_NAME	Char	6	13	User name..
USEIM_LDAPPROF	Char	15	260	EIM LDAPBIND profile name.

Data Set Record Formats

The records associated with data sets are:

- Data Set Basic Data
- Data Set Categories

Database Unload—IRRDBU00

- Data Set Conditional Access
- Data Set Volumes
- Data Set Access
- Data Set Installation Data
- Data Set DFP Data
- Data Set TME Data Record

Data Set Basic Data Record (0400): The Data Set Basic Data record defines the basic information for a data set. There is one record per data set profile.

Table 194. Data Set Basic Data Record. Defines the basic information about a data set.

Field Name	Type	Position		Comments
		Start	End	
DSBD_RECORD_TYPE	Int	1	4	Record type of the Data Set Basic Data record (0400).
DSBD_NAME	Char	6	49	Data set name as taken from the profile name.
DSBD_VOL	Char	51	56	Volume upon which this data set resides. Blank if the profile is generic, and *MODEL if the profile is a model profile.
DSBD_GENERIC	Yes/No	58	61	Is this a generic profile?
DSBD_CREATE_DATE	Date	63	72	Date the profile was created.
DSBD_OWNER_ID	Char	74	81	The user ID or group name which owns the profile.
DSBD_LASTREF_DATE	Date	83	92	The date that the data set was last referenced.
DSBD_LASTCHG_DATE	Date	94	103	The date that the data set was last changed.
DSBD_ALTER_CNT	Int	105	109	The number of times that the data set was accessed with ALTER authority.
DSBD_CONTROL_CNT	Int	111	115	The number of times that the data set was accessed with CONTROL authority.
DSBD_UPDATE_CNT	Int	117	121	The number of times that the data set was accessed with UPDATE authority.
DSBD_READ_CNT	Int	123	127	The number of times that the data set was accessed with READ authority.
DSBD_UACC	Char	129	136	The universal access of this data set. Valid values are NONE, EXECUTE, READ, UPDATE, CONTROL, and ALTER.
DSBD_GRPDS	Yes/No	138	141	Is this a group data set?
DSBD_AUDIT_LEVEL	Char	143	150	Indicates the level of resource-owner-specified auditing that is performed. Valid values are ALL, SUCCESS, FAIL, and NONE.
DSBD_GRP_ID	Char	152	159	The connect group of the user who created this data set.
DSBD_DS_TYPE	Char	161	168	The type of the data set. Valid values are VSAM, NONVSAM, TAPE, and MODEL.
DSBD_LEVEL	Int	170	172	The level of the data set.
DSBD_DEVICE_NAME	Char	174	181	The EBCDIC name of the device type on which the data set resides.
DSBD_GAUDIT_LEVEL	Char	183	190	Indicates the level of auditor-specified auditing that is performed. Valid values are ALL, SUCCESS, FAIL, and NONE.
DSBD_INSTALL_DATA	Char	192	446	Installation-defined data.
DSBD_AUDIT_OKQUAL	Char	448	455	The resource-owner-specified successful access audit qualifier. This is set to blanks if AUDIT_LEVEL is NONE. Otherwise, it is set to either READ, UPDATE, CONTROL, or ALTER.
DSBD_AUDIT_FAQUAL	Char	457	464	The resource-owner-specified failing access audit qualifier. This is set to blanks if AUDIT_LEVEL is NONE. Otherwise, it is set to either READ, UPDATE, CONTROL, or ALTER.

Table 194. Data Set Basic Data Record (continued). Defines the basic information about a data set.

Field Name	Type	Position		Comments
		Start	End	
DSBD_GAUDIT_OKQUAL	Char	466	473	The auditor-specified successful access audit qualifier. This is set to blanks if GAUDIT_LEVEL is NONE. Otherwise, it is set to either READ, UPDATE, CONTROL, or ALTER.
DSBD_GAUDIT_FAQUAL	Char	475	482	The auditor-specified failing access audit qualifier. This is set to blanks if GAUDIT_LEVEL is NONE. Otherwise, it is set to either READ, UPDATE, CONTROL, or ALTER.
DSBD_WARNING	Yes/No	484	487	Does this data set have the WARNING attribute?
DSBD_SECLEVEL	Int	489	491	The data set security level.
DSBD_NOTIFY_ID	Char	493	500	User ID that is notified when violations occur.
DSBD_RETENTION	Int	502	506	Retention period of the data set.
DSBD_ERASE	Yes/No	508	511	For a DASD data set, is this data set scratched when the data set is deleted?
DSBD_SECLABEL	Char	513	520	Security label of the data set.

Data Set Categories Record (0401): The Data Set Categories record defines the categories to which a data set belongs. There is one record per data set/category combination.

Table 195. Data Set Categories Record. Defines the categories with which a data set is associated.

Field Name	Type	Position		Comments
		Start	End	
DSCAT_RECORD_TYPE	Int	1	4	Record type of the Data Set Categories record (0401).
DSCAT_NAME	Char	6	49	Data set name as taken from the profile name.
DSCAT_VOL	Char	51	56	Volume upon which this data set resides. Blank if the profile is generic, and *MODEL if the profile is a model profile.
DSCAT_CATEGORY	Int	58	62	Category associated with this data set.

Data Set Conditional Access Record (0402): The Data Set Conditional Access record defines the data sets which have conditional access permissions. There is one record per data set/access combination.

Table 196. Data Set Conditional Access Record. Defines the conditional access element/user access combinations for a data set.

Field Name	Type	Position		Comments
		Start	End	
DSCACC_RECORD_TYPE	Int	1	4	Record type of the Data Set Conditional Access record (0402).
DSCACC_NAME	Char	6	49	Data set name as taken from the profile name.
DSCACC_VOL	Char	51	56	Volume upon which this data set resides. Blank if the profile is generic, and *MODEL if the profile is a model profile.
DSCACC_CATTYPE	Char	58	65	The type of conditional access checking that is being performed. Valid values are APPCPOR, PROGRAM, CONSOLE, TERMINAL and JESINPUT.
DSCACC_CANAME	Char	67	74	The name of a conditional access element which is permitted access.
DSCACC_AUTH_ID	Char	76	83	The user ID or group name that is authorized to the data set.

Database Unload—IRRDBU00

Table 196. Data Set Conditional Access Record (continued). Defines the conditional access element/user access combinations for a data set.

Field Name	Type	Position		Comments
		Start	End	
DSCACC_ACCESS	Char	85	92	The access of the conditional access element/user combination. Valid values are NONE, EXECUTE, READ, UPDATE, CONTROL, and ALTER.
DSCACC_ACCESS_CNT	Int	94	98	The number of times that the data set was accessed.
DSCACC_NET_ID	Char	100	107	The network name when DSCACC_CATYPE is APPCPORT.

Data Set Volumes Record (0403): The Data Set Volumes record defines the volumes upon which a data set resides. There is one record per data set/volume combination. Records exist in this table only for discrete data set profiles.

Table 197. Data Set Volumes Record. Defines the volumes upon which a data set resides.

Field Name	Type	Position		Comments
		Start	End	
DSVOL_RECORD_TYPE	Int	1	4	Record type of the Data Set Volumes record (0403).
DSVOL_NAME	Char	6	49	Data set name as taken from the profile name.
DSVOL_VOL	Char	51	56	Volume upon which this data set resides.
DSVOL_VOL_NAME	Char	58	63	A volume upon which the data set resides.

Data Set Access Record (0404): The Data Set Access record defines the users or groups which are allowed to access data. There is one record per data set/authorization combination.

Table 198. Data Set Access Record. Defines the authorizations and access counts for data sets.

Field Name	Type	Position		Comments
		Start	End	
DSACC_RECORD_TYPE	Int	1	4	Record type of the Data Set Access Record (0404).
DSACC_NAME	Char	6	49	Data set name as taken from the profile name.
DSACC_VOL	Char	51	56	Volume upon which this data set resides. Blank if the profile is generic, and *MODEL if the profile is a model profile.
DSACC_AUTH_ID	Char	58	65	The user ID or group name that is authorized to the data set.
DSACC_ACCESS	Char	67	74	The access allowed to the user. Valid values are NONE, EXECUTE, READ, UPDATE, CONTROL, and ALTER.
DSACC_ACCESS_CNT	Int	76	80	The number of times that the data set was accessed.

Data Set Installation Data Record (0405): The Data Set Installation Data record defines the user data that is associated with a data set profile. There is one record per data set/installation data combination.

This record type contains the data stored in the USRCNT repeat group, which is a field in the RACF database that is reserved for your installation's use. None of the RACF commands manipulate this field. Do not confuse this field with the DSBD_INSTALL_DATA field, shown in Table 194 on page 276, which you enter into the database using the ADDSD and ALTDSD commands.

Table 199. Data Set Installation Data Record. Defines the user-specified information associated with a data set.

Field Name	Type	Position		Comments
		Start	End	
DSINSTD_RECORD_TYPE	Int	1	4	Record type of the Data Set Installation Data Record (0405).
DSINSTD_NAME	Char	6	49	Data set name as taken from the profile name.
DSINSTD_VOL	Char	51	56	Volume upon which this data set resides. Blank if the profile is generic, and *MODEL if the profile is a model profile.
DSINSTD_USR_NAME	Char	58	65	The name of the installation-defined field.
DSINSTD_USR_DATA	Char	67	321	The data for the installation-defined field.
DSINSTD_USR_FLAG	Char	323	330	The flag for the installation-defined field in the form X<cc>.

Data Set DFP Data Record (0410): The Data Set DFP Data record defines the DFP information required by the System Managed Storage (SMS) facility of the Data Facility Product (DFP). There is one record per data set/DFP data combination.

Table 200. Data Set DFP Data Record. Defines the SMS Data that is associated with a data set.

Field Name	Type	Position		Comments
		Start	End	
DSDFP_RECORD_TYPE	Int	1	4	Record type of the Data Set DFP Data record (0410).
DSDFP_NAME	Char	6	49	Data set name as taken from the profile name.
DSDFP_VOL	Char	51	56	Volume upon which this data set resides. Blank if the profile is generic, and *MODEL if the profile is a model profile.
DSDFP_RESOWNER_ID	Char	58	65	The resource owner of the data set.

Data Set TME Role Record (0421): The Data Set TME role record identifies ROLE profiles and access authorities referencing the data set. There is one record per data set/role combination.

Table 201. Data Set TME Data Record

Field Name	Type	Position		Comments
		Start	End	
DSTME_RECORD_TYPE	Int	1	4	Record type of the Data Set TME Data Record (0421).
DSTME_NAME	Char	6	49	Data set name as taken from the profile name.
DSTME_VOL	Char	51	56	Volume upon which this data set resides. Blank if the profile is generic, and *MODEL if the profile is a model profile.
DSTME_ROLE_NAME	Char	58	303	Role profile name.
DSTME_ACCESS_AUTH	Char	305	312	Access permission to this resource as defined by the role.
DSTME_COND_CLASS	Char	314	321	Class name for conditional access.
DSTME_COND_PROF	Char	323	568	Resource profile for conditional access.

General Resource Record Formats

The records associated with general resources are:

- General Resource Basic Data
- General Resource Tape Volume Data
- General Resource Categories
- General Resource Members
- General Resource Volumes

Database Unload—IRRDBU00

- General Resource Access
- General Resource Installation Data
- General Resource Conditional Access Data
- General Resource Filter Data Record
- General Resource Session Data
- General Resource Session Entities
- General Resource DLF Data
- General Resource DLF Job Names
- General Resource Started Task Data
- General Resource SystemView Data
- General Resource Certificate Data Record
- General Resource Certificate Reference Record
- General Resource Key Ring Data Record
- General Resource TME Data Record
- General Resource TME Child Record
- General Resource TME Resource Record
- General Resource TME Group Record
- General Resource TME Role Record
- General Resource KERB Data Record
- General Resource PROXY Data Record
- General Resource EIM Data Record

Note: The digital certificates stored in the CERTDATA segment of general resource profiles are not readable text. Therefore, RACF bypasses the unload of the CERTDATA segment, and there is no record for this data.

General Resource Basic Data Record (0500): The General Resource Basic Data record defines the basic information about a general resource. There is one record per general resource profile.

Table 202. General Resource Basic Data Record. Defines the basic information about a general resource.

Field Name	Type	Position		Comments
		Start	End	
GRBD_RECORD_TYPE	Int	1	4	Record type of the General Resource Basic Data record (0500).
GRBD_NAME	Char	6	251	General resource name as taken from the profile name.
GRBD_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs.
GRBD_GENERIC	Yes/No	262	265	Is this a generic profile?
GRBD_CLASS	Int	267	269	The class number of the profile.
GRBD_CREATE_DATE	Date	271	280	Date the profile was created.
GRBD_OWNER_ID	Char	282	289	The user ID or group name which owns the profile.
GRBD_LASTREF_DATE	Date	291	300	The date that the resource was last referenced.
GRBD_LASTCHG_DATE	Date	302	311	The date that the resource was last changed.
GRBD_ALTER_CNT	Int	313	317	The number of times that the resource was accessed with ALTER authority.
GRBD_CONTROL_CNT	Int	319	323	The number of times that the resource was accessed with CONTROL authority.
GRBD_UPDATE_CNT	Int	325	329	The number of times that the resource was accessed with UPDATE authority.
GRBD_READ_CNT	Int	331	335	The number of times that the resource was accessed with READ authority.

Table 202. General Resource Basic Data Record (continued). Defines the basic information about a general resource.

Field Name	Type	Position		Comments
		Start	End	
GRBD_UACC	Char	337	344	The universal access of this resource. For profiles in classes other than DIGTCERT, the valid values are NONE, READ, EXECUTE, UPDATE, CONTROL, and ALTER. For DIGTCERT profiles, the valid values are TRUST, NOTRUST, and HIGHTRST.
GRBD_AUDIT_LEVEL	Char	346	353	Indicates the level of resource-owner-specified auditing that is performed. Valid values are ALL, SUCCESS, FAIL, and NONE.
GRBD_LEVEL	Int	355	357	The level of the resource.
GRBD_GAUDIT_LEVEL	Char	359	366	Indicates the level of auditor-specified auditing that is performed. Valid values are ALL, SUCCESS, FAIL, and NONE.
GRBD_INSTALL_DATA	Char	368	622	Installation-defined data.
GRBD_AUDIT_OKQUAL	Char	624	631	The resource-owner-specified successful access audit qualifier. This is set to blanks if AUDIT_LEVEL is NONE. Otherwise, it is set to either READ, UPDATE, CONTROL, or ALTER.
GRBD_AUDIT_FAQUAL	Char	633	640	The resource-owner-specified failing access audit qualifier. This is set to blanks if AUDIT_LEVEL is NONE. Otherwise, it is set to either READ, UPDATE, CONTROL, or ALTER.
GRBD_GAUDIT_OKQUAL	Char	642	649	The auditor-specified successful access audit qualifier. This is set to blanks if GAUDIT_LEVEL is NONE. Otherwise, it is set to either READ, UPDATE, CONTROL, or ALTER.
GRBD_GAUDIT_FAQUAL	Char	651	658	The auditor-specified failing access audit qualifier. This is set to blanks if GAUDIT_LEVEL is NONE. Otherwise, it is set to either READ, UPDATE, CONTROL, or ALTER.
GRBD_WARNING	Yes/No	660	663	Does this resource have the WARNING attribute?
GRBD_SINGLEDSD	Yes/No	665	668	If this is a TAPEVOL profile, is there only one data set on this tape?
GRBD_AUTO	Yes/No	670	673	If this is a TAPEVOL profile, is the TAPEVOL protection automatic?
GRBD_TVTOC	Yes/No	675	678	If this is a TAPEVOL profile, is there a tape volume table of contents on this tape?
GRBD_NOTIFY_ID	Char	680	687	User ID that is notified when violations occur.
GRBD_ACCESS_SUN	Yes/No	689	692	Can the terminal be used on Sunday?
GRBD_ACCESS_MON	Yes/No	694	697	Can the terminal be used on Monday?
GRBD_ACCESS_TUE	Yes/No	699	702	Can the terminal be used on Tuesday?
GRBD_ACCESS_WED	Yes/No	704	707	Can the terminal be used on Wednesday?
GRBD_ACCESS_THU	Yes/No	709	712	Can the terminal be used on Thursday?
GRBD_ACCESS_FRI	Yes/No	714	717	Can the terminal be used on Friday?
GRBD_ACCESS_SAT	Yes/No	719	722	Can the terminal be used on Saturday?
GRBD_START_TIME	Time	724	731	After what time may a user logon from this terminal?
GRBD_END_TIME	Time	733	740	After what time may a user not logon from this terminal?
GRBD_ZONE_OFFSET	Char	742	746	Time zone in which the terminal is located. Expressed as hh:mm. Blank if the time zone has not been specified.
GRBD_ZONE_DIRECT	Char	748	748	The direction of the time zone shift. Valid values are E(east), W(west), and blank.
GRBD_SECLEVEL	Int	750	752	The security level of the general resource.
GRBD_APPL_DATA	Char	754	1,008	Installation-defined data.
GRBD_SECLABEL	Char	1,010	1,017	The security label for the general resource.

Database Unload—IRRDBU00

General Resource Tape Volume Data Record (0501): The General Resource Tape Volume Data Record defines the characteristics of the tape volume upon which a data set resides. There is one record per general resource/tape volume combination.

Table 203. General Resource Tape Volume Record. Defines the characteristics of a tape volume.

Field Name	Type	Position		Comments
		Start	End	
GRTVOL_RECORD_TYPE	Int	1	4	Record type of the General Resource Tape Volume Data record (0501).
GRTVOL_NAME	Char	6	251	General resource name as taken from the profile name.
GRTVOL_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs, namely TAPEVOL.
GRTVOL_SEQUENCE	Int	262	266	The file sequence number of the tape data set.
GRTVOL_CREATE_DATE	Date	268	277	Creation date of the tape data set.
GRTVOL_DISCRETE	Yes/No	279	282	Does a discrete profile exist?
GRTVOL_INTERN_NAME	Char	284	327	The RACF internal data set name.
GRTVOL_INTERN_VOLS	Char	329	583	The volumes upon which the data set resides.
GRTVOL_CREATE_NAME	Char	585	628	The data set name used when creating the data set.

General Resource Categories Record (0502): The General Resource Categories record defines the categories associated with a general resource. There is one record per general resource/category combination.

Table 204. General Resource Categories Record. Defines the categories associated with a general resource.

Field Name	Type	Position		Comments
		Start	End	
GRCAT_RECORD_TYPE	Int	1	4	Record type of the General Resources Categories record (0502).
GRCAT_NAME	Char	6	251	General resource name as taken from the profile name.
GRCAT_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs.
GRCAT_CATEGORY	Int	262	266	Category to which this general resource belongs.

General Resource Members Record (0503): The General Resource Members record defines the members of a general resource profile group. There is one record per general resource/member combination.

Table 205. General Resource Members Record. Defines the members of a general resource.

Field Name	Type	Position		Comments
		Start	End	
GRMEM_RECORD_TYPE	Int	1	4	Record type of the General Resource Members record (0503).
GRMEM_NAME	Char	6	251	General resource name as taken from the profile name.
GRMEM_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs.

Table 205. General Resource Members Record (continued). Defines the members of a general resource.

Field Name	Type	Position		Comments
		Start	End	
GRMEM_MEMBER	Char	262	516	Member value for this general resource. <ul style="list-style-type: none"> For VMXEVENT profiles, this is the element that is being audited. For PROGRAM profiles, this is the name of the data set which contains the program. For GLOBAL profiles, this is the name of the resource for which a global access applies. For SECDATA security level (SECLEVEL) profiles, this is the level name. For SECDATA CATEGORY profiles, this is the category name. For NODES profiles, this is the user ID, group name, and SECLABEL translation data.
GRMEM_GLOBAL_ACC	Char	518	525	If this is a GLOBAL profile, this is the access that is allowed. Valid values are NONE, READ, UPDATE, CONTROL, and ALTER.
GRMEM_PADS_DATA	Char	527	534	If this is a PROGRAM profile, this field contains the Program Access to Data Set (PADS) information for the profile. Valid values are PADCHK and NOPADCHK.
GRMEM_VOL_NAME	Char	536	541	If this is a PROGRAM profile, this field defines the volume upon which the program resides.
GRMEM_VMEVENT_DATA	Char	543	547	If this is a VMXEVENT profile, this field defines the level of auditing that is being performed. Valid values are CTL, AUDIT, and NOCTL.
GRMEM_SECLEVEL	Int	549	553	If this is a SECLEVEL profile in the SECDATA class, this is the numeric security level that is associated with the SECLEVEL.
GRMEM_CATEGORY	Int	555	559	If this is a CATEGORY profile in the SECDATA class, this is the numeric category that is associated with the CATEGORY.

General Resource Volumes Record (0504): The General Resource Volumes record defines the volumes in a tape volume set. There is one record per tape volume set/volume combination.

Table 206. General Resource Volumes Record. Defines the volumes in a tape volume set.

Field Name	Type	Position		Comments
		Start	End	
GRVOL_RECORD_TYPE	Int	1	4	Record type of the General Resources Volumes record (0504).
GRVOL_NAME	Char	6	251	General resource name as taken from the profile name.
GRVOL_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs, namely TAPEVOL.
GRVOL_VOL_NAME	Char	262	267	Name of a volume in a tape volume set.

General Resource Access Record (0505): The General Resource Access record defines the users or groups who have specific access to general resources. There is one record per general resource/authorization combination.

Table 207. General Resource Access Record. Defines the authorizations to general resources.

Field Name	Type	Position		Comments
		Start	End	
GRACC_RECORD_TYPE	Int	1	4	Record type of the General Resource Access record (0505).

Database Unload—IRRDBU00

Table 207. General Resource Access Record (continued). Defines the authorizations to general resources.

Field Name	Type	Position		Comments
		Start	End	
GRACC_NAME	Char	6	251	General resource name as taken from the profile name.
GRACC_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs.
GRACC_AUTH_ID	Char	262	269	User ID or group name which is authorized to use the general resource.
GRACC_ACCESS	Char	271	278	The authority that the user or group has over the resource. Valid values are NONE, READ, UPDATE, CONTROL, and ALTER.
GRACC_ACCESS_CNT	Int	280	284	The number of times that the resource was accessed.

General Resource Installation Data Record (0506): The General Resource Installation Data record defines the user data associated with a general resource. There is one record per general resource/data combination.

This record type contains data stored in the USRCNT repeat group, which is a field in the RACF database that is reserved for your installation's use. None of the RACF commands manipulate this field. Do not confuse this field with the GRBD_INSTALL_DATA field, shown in Table 202 on page 280, which you enter into the database using the RDEFINE and RALTER commands.

Table 208. General Resource Installation Data Record. Defines the user-specified data associated with a general resource.

Field Name	Type	Position		Comments
		Start	End	
GRINSTD_RECORD_TYPE	Int	1	4	Record type of the General Resource Installation Data record (0506).
GRINSTD_NAME	Char	6	251	General resource name as taken from the profile name.
GRINSTD_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs.
GRINSTD_USR_NAME	Char	262	269	The name of the installation-defined field.
GRINSTD_USR_DATA	Char	271	525	The data for the installation-defined field.
GRINSTD_USR_FLAG	Char	527	534	The flag for the installation-defined field in the form X<nn>.

General Resource Conditional Access Record (0507): The General Resource Conditional Access record defines the conditional access to a general resource. There is one record per general resource/access combination.

Table 209. General Resource Conditional Access Record. Defines the conditional access for a general resource.

Field Name	Type	Position		Comments
		Start	End	
GRCACC_RECORD_TYPE	Int	1	4	Record type of the General Resources Conditional Access record (0507).
GRCACC_NAME	Char	6	251	General resource name as taken from the profile name.
GRCACC_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs.
GRCACC_CATYPE	Char	262	269	The type of conditional access checking that is being performed. Valid values are CONSOLE, TERMINAL, JESINPUT, SYSID, and APPCPORT.
GRCACC_CANAME	Char	271	278	The name of a conditional access element which is permitted access.

Table 209. General Resource Conditional Access Record (continued). Defines the conditional access for a general resource.

Field Name	Type	Position		Comments
		Start	End	
GRCACC_AUTH_ID	Char	280	287	The user ID or group name which has authority to the general resource.
GRCACC_ACCESS	Char	289	296	The authority of the conditional access element/user combination. Valid values are NONE, READ, UPDATE, CONTROL, and ALTER.
GRCACC_ACCESS_CNT	Int	298	302	The number of times that the general resource was accessed.
GRCACC_NET_ID	Char	304	311	The network name when GRCACC_CATYPE is APPCPORT.

General Resource Filter Data Record (0508): The General Resource Filter Data record defines the information used to create the filter described by this DIGTNMAP profile and identifies the associated user ID or criteria (DIGTCRIT) profile.

Table 210. General Resource Filter Data Record. Defines the certificate mapping information associated with a DIGTNMAP profile.

Field Name	Type	Position		Comments
		Start	End	
GRFLTR_RECORD_TYPE	Int	1	4	Record Type of the Filter Data record (0508).
GRFLTR_NAME	Char	6	251	General resource name as taken from the profile name.
GRFLTR_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs.
GRFLTR_LABEL	Char	262	293	The label associated with this filter.
GRFLTR_STATUS	Char	295	302	The status of this filter (TRUST) for filters that are trusted.
GRFLTR_USER	Char	304	549	The user ID or criteria profile name associated with this filter.
GRFLTR_CREATE_NAME	Char	551	1061	The issuer's and/ or subject's name used to create this profile.

General Resource Session Data Record (0510): The General Resource Session Data record defines the session data associated with a general resource. There is one record per APPCLU profile.

Table 211. General Resource Session Data Record. Defines the session data associated with an APPCLU profile.

Field Name	Type	Position		Comments
		Start	End	
GRSES_RECORD_TYPE	Int	1	4	Record type of the General Resources Session Data record (0510).
GRSES_NAME	Char	6	251	General resource name as taken from the profile name.
GRSES_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs, namely APPCLU.
GRSES_SESSION_KEY	Char	262	269	The key associated with the APPC session.
GRSES_LOCKED	Yes/No	271	274	Is the profile locked?
GRSES_KEY_DATE	Date	276	285	Last date that the session key was changed.
GRSES_KEY_INTERVAL	Int	287	291	Number of days that the key is valid.
GRSES_SLS_FAIL	Int	293	297	Current number of failed attempts.
GRSES_MAX_FAIL	Int	299	303	Number of failed attempts before lockout.

Database Unload—IRRDBU00

Table 211. General Resource Session Data Record (continued). Defines the session data associated with an APPCLU profile.

Field Name	Type	Position		Comments
		Start	End	
GRSES_CONVSEC	Char	305	312	Specifies the security checking performed when sessions are established. Valid values are NONE, CONVSEC, PERSISTV, ALREADYV, and AVPV.

General Resource Session Entities (0511): The General Resource Session Entities record defines the entities associated with a general resource APPCLU profile. There is one record per APPCLU profile/session entity combination.

Table 212. General Resource Session Entity Record. Defines the session entities data associated with a general resource APPCLU profile.

Field Name	Type	Position		Comments
		Start	End	
GRSESE_RECORD_TYPE	Int	1	4	Record type of the General Resources Session Entities record (0511).
GRSESE_NAME	Char	6	251	General resource name as taken from the profile name.
GRSESE_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs, namely APPCLU.
GRSESE_ENTITY_NAME	Char	262	296	Entity name.
GRSES_FAIL_CNT	Int	298	302	The number of failed session attempts.

General Resource DLF Data Record (0520): The General Resource DLF Data record defines the Data Lookaside Facility (DLF) data associated with a general resource. There is one record per general resource/DLF data combination.

Table 213. General Resource DLF Data Record. Defines the DLF data associated with a general resource.

Field Name	Type	Position		Comments
		Start	End	
GRDLF_RECORD_TYPE	Int	1	4	Record type of the General Resources DLF Data record (0520).
GRDLF_NAME	Char	6	251	General resource name as taken from the profile name.
GRDLF_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs, namely DLFCCLASS.
GRDLF_RETAIN	Yes/No	262	265	Is this a retained resource?

General Resource DLF Job Names Record (0521): The General Resource DLF Job Names record defines the job names associated with a DLF general resource. There is one record per general resource/DLF job name combination.

Table 214. General Resource DLF Job Names Record. Defines the DLF job name data about a DLF general resource.

Field Name	Type	Position		Comments
		Start	End	
GRDLFJ_RECORD_TYPE	Int	1	4	Record type of the General Resources DLF Job Names record (0521).
GRDLFJ_NAME	Char	6	251	General resource name as taken from the profile name.
GRDLFJ_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs, namely DLFCCLASS.
GRDLFJ_JOB_NAME	Char	262	269	The job name associated with the general resource.

General Resource Started Task Data Record (0540): The General Resource Started Task Data Record defines the information associated with the definition of a started task in the STARTED general resource class.

Table 215. General Resource Started Task Data Record. Records STDATA information associated with a general resource.

Field Name	Type	Position		Comments
		Start	End	
GRST_RECORD_TYPE	Int	1	4	Record type (0540).
GRST_NAME	Char	6	251	Profile name.
GRST_CLASS_NAME	Char	253	260	The class name, STARTED.
GRST_USER_ID	Char	262	269	User ID assigned.
GRST_GROUP_ID	Char	271	278	Group name assigned.
GRST_TRUSTED	Yes/No	280	283	Is process to run trusted?
GRST_PRIVILEGED	Yes/No	285	288	Is process to run privileged?
GRST_TRACE	Yes/No	290	293	Is entry to be traced?

General Resource SystemView Data Record (0550): The General Resource SystemView Data Record defines the information associated with the SYSMVIEW general resource class.

Table 216. General Resource SystemView Data Record. Defines the information associated with the SYSMVIEW general resource class.

Field Name	Type	Position		Comments
		Start	End	
GRSV_RECORD_TYPE	Int	1	4	Record type (0550).
GRSV_NAME	Char	6	251	Profile name.
GRSV_CLASS_NAME	Char	253	260	Class name, SYSMVIEW.
GRSV_SCRIPT_NAME	Char	262	269	Logon script name for the application.
GRSV_PARM_NAME	Char	271	278	Parameter list name for the application.

General Resource Certificate Data Record (0560): The General Resource Certificate Data Record defines the information associated with the Certificate Data Record resource class.

Table 217. General Resource Certificate Data Record. Defines the information associated with the Certificate Data Record resource class.

Field Name	Type	Position		Comments
		Start	End	
GRCERT_RECORD_TYPE	Int	1	4	Record type of the Certificate Data record(0560).
GRCERT_NAME	Char	6	251	General resource name as taken from the profile name.
GRCERT_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs.
GRCERT_START_DATE	Date	262	271	The date from which this certificate is valid.
GRCERT_START_TIME	Time	273	280	The time from which this certificate is valid.
GRCERT_END_DATE	Date	282	291	The date after which this certificate is no longer valid.
GRCERT_END_TIME	Time	293	300	The time after which this certificate is no longer valid.
GRCERT_KEY_TYPE	Char	302	309	The type of private key associated with the certificate. Valid values are <i>PKCSDER</i> , <i>ICSFTOKN</i> , <i>PCICCTKN</i> or all blanks to indicate no private key.

Database Unload—IRRDBU00

Table 217. General Resource Certificate Data Record (continued). Defines the information associated with the Certificate Data Record resource class.

Field Name	Type	Position		Comments
		Start	End	
GRCERT_KEY_SIZE	Int	311	320	The size of private key associated with the certificate, expressed in bits.
GRCERT_LAST_SERIAL	Char	322	337	The hexadecimal representation of the low-order eight bytes of the serial number of the last certificate signed with this key.
GRCERT_RING_SEQN	Int	339	348	A sequence number for certificates within the ring.

General Resource Certificate References Record (0561): The General Resource Certificate References Record defines the information associated with the Certificate References Record resource class.

Table 218. General Resource Certificate References Record. Defines the information associated with the Certificate References Data Record resource class.

Field Name	Type	Position		Comments
		Start	End	
CERTR_RECORD_TYPE	Int	1	4	Record type of the Certificate Reference record(0561).
CERTR_NAME	Char	6	251	General resource name as taken from the profile name.
CERTR_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs.
CERTR_RING_NAME	Char	262	507	The name of the profile which represents a key ring with which this certificate is associated.

General Resource Key Ring Data Record (0562): The General Resource Key Ring Data Record defines the information associated with the Key Ring Data Record resource class.

Table 219. General Resource Key Ring Data Record. Defines the information associated with the Key Ring Data Record resource class.

Field Name	Type	Position		Comments
		Start	End	
KEYR_RECORD_TYPE	Int	1	4	Record type of the Key Ring Data record(0562).
KEYR_NAME	Char	6	251	General resource name as taken from the profile name.
KEYR_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs.
KEYR_CERT_NAME	Char	262	507	The name of the profile which contains the certificate which is in this key ring.
KEYR_CERT_USAGE	Char	509	516	The usage of the certificate within the ring. Valid values are <i>PERSONAL</i> , <i>SITE</i> and, <i>CERTAUTH</i> .
KEYR_CERT_DEFAULT	Yes/No	518	521	Is this certificate the default certificate within the ring?
KEYR_CERT_LABEL	Char	523	554	The label associated with the certificate.

General Resource TME Data Record (0570): The General Resource TME data record identifies the parent ROLE profile from which this profile inherits attributes. There is one record per general resource profile/TME data combination.

Table 220. General Resource TME Data Record

Field Name	Type	Position		Comments
		Start	End	
GRTME_RECORD_TYPE	Int	1	4	Record type of the general resource TME data record (0570).
GRTME_NAME	Char	6	251	General resource name as taken from the profile name.
GRTME_CLASS_NAME	Char	253	260	Name of the class to which the general resource belongs.
GRTME_PARENT	Char	262	507	Parent role.

General Resource TME Child Record (0571): The general resource TME child record identifies a ROLE profile which inherits attributes from this profile. There is one record per general resource/child combination.

Table 221. General Resource TME Child Record

Field Name	Type	Position		Comments
		Start	End	
GRTMEC_RECORD_TYPE	Int	1	4	Record type of the general resource TME child record (0571).
GRTMEC_NAME	Char	6	251	General resource name as taken from the profile name.
GRTMEC_CLASS_NAME	Char	253	260	Name of the class to which the general resource belongs.
GRTMEC_CHILD	Char	262	507	Child role.

General Resource TME Resource Record (0572): The general resource TME resource record identifies resources and access authorities for groups defined in the role. There is one record per general resource/resource combination.

Table 222. General Resource TME Resource Record

Field Name	Type	Position		Comments
		Start	End	
GRTMER_RECORD_TYPE	Int	1	4	Record type of the general resource TME resource record (0572).
GRTMER_NAME	Char	6	251	General resource name as taken from the profile name.
GRTMER_CLASS_NAME	Char	253	260	Name of the class to which the general resource belongs.
GRTMER_ORIGIN_ROLE	Char	262	507	Role profile from which resource access is inherited.
GRTMER_PROF_CLASS	Char	509	516	Class name of the origin-role resource.
GRTMER_PROF_NAME	Char	518	763	Resource name defined in the origin role.
GRTMER_ACCESS_AUTH	Char	765	772	Access permission to the resource.
GRTMER_COND_CLASS	Char	774	781	Class name for conditional access.
GRTMER_COND_PROF	Char	783	1028	Resource profile for conditional access.

General Resource TME Group Record (0573): The general resource TME group record identifies groups that are permitted to resources in the role. There is one record per general resource/group combination.

Table 223. General Resource TME Group Record

Field Name	Type	Position		Comments
		Start	End	
GRTMEG_RECORD_TYPE	Int	1	4	Record type of the general resource TME group record (0573).
GRTMEG_NAME	Char	6	251	General resource name as taken from the profile name.

Database Unload—IRRDBU00

Table 223. General Resource TME Group Record (continued)

Field Name	Type	Position		Comments
		Start	End	
GRTMEG_CLASS_NAME	Char	253	260	Name of the class to which the general resource belongs.
GRTMEG_GROUP	Char	262	269	Group name defined to the role.

General Resource TME Role Record (0574): The general resource TME role record identifies ROLE profiles and access authorities referencing the general resource. There is one record per general resource/role combination.

Table 224. General Resource TME Role Record

Field Name	Type	Position		Comments
		Start	End	
GRTMEE_RECORD_TYPE	Int	1	4	Record type of the general resource TME role record (0574).
GRTMEE_NAME	Char	6	251	General resource name as taken from the profile name.
GRTMEE_CLASS_NAME	Char	253	260	Name of the class to which the general resource belongs.
GRTMEE_ROLE_NAME	Char	262	507	Role profile name.
GRTMEE_ACCESS_AUTH	Char	509	516	Access permission to this resource as defined by the role.
GRTMEE_COND_CLASS	Char	518	525	Class name for conditional access.
GRTMEE_COND_PROF	Char	527	772	Resource profile for conditional access.

General Resource KERB Data Record (0580): The general resource KERB Data record defines the Kerberos information for a realm. There is only one record per general resource profile that contains a KERB segment.

Table 225. General Resource KERB Data Record

Field Name	Type	Position		Comments
		Start	End	
GRKERB_RECORD_TYPE	Int	1	4	Record type of the general resource KERB segment record (0580).
GRKERB_NAME	Char	6	251	General resource name as taken from the profile name.
GRKERB_CLASS_NAME	Char	253	260	Name of the class to which the general resource profile belongs.
GRKERB_KERBNAME	Char	262	501	The Kerberos realm name.
GRKERB_MIN_LIFE	Int	503	512	Minimum ticket life.
GRKERB_MAX_LIFE	Int	514	523	Maximum ticket life.
GRKERB_DEF_LIFE	Int	525	534	Default ticket life.
GRKERB_KEY_VERS	Int	536	538	Current key version.
GRKERB_ENCRYPT_DES	Yes/No	540	543	Key encryption using DES is enabled.
GRKERB_ENCRYPT_DES3	Yes/No	545	548	Key encryption using DES3 is enabled.
GRKERB_ENCRYPT_DESD	Yes/No	550	553	Key encryption using DES with derivation is enabled.

General Resource PROXY Record (0590): The general resource PROXY record identifies default information related to the LDAP proxy for a general resource. There is only one record per general resource profile that contains a PROXY segment.

Table 226. General Resource PROXY Record

Field Name	Type	Position		Comments
		Start	End	
GRPROXY_RECORD_TYPE	Int	1	4	Record type of the general resource PROXY record (0590).
GRPROXY_NAME	Char	6	251	General resource name as taken from the profile name.
GRPROXY_CLASS_NAME	Char	253	260	Name of the class to which the general resource belongs.
GRPROXY_LDAP_HOST	Char	262	1284	LDAP server URL.
GRPROXY_BIND_DN	Char	1286	2308	LDAP BIND distinguished name.

| **General Resource EIM Record (05A0):** The general resource EIM record defines EIM-related information. There is only one record per general resource profile that contains an EIM segment.

Table 227. General Resource PROXY Record

Field Name	Type	Position		Comments
		Start	End	
GREIM_RECORD_TYPE	Int	1	4	Record type of the general resource EIM segment record (05A0).
GREIM_NAME	Char	6	251	Profile name.
GREIM_CLASS_NAME	Char	253	260	Class name.
GREIM_DOMAIN_DN	Char	262	1284	EIM domain name.
GRPROXY_ENABLE	Char	1286	2286	EIM Enable option.
GRPROXY_LOCALREG	Char	1366	1620	EIM LDAP local registry name.

Database Unload—IRRDBU00

Chapter 11. The RACF Secured Signon PassTicket

The RACF secured signon function provides an alternative to the RACF password called a *PassTicket*. The RACF PassTicket is a *one-time-only* password that is generated by a requesting product or function. It is an alternative to the RACF password that removes the need to send RACF passwords across the network in clear text. It makes it possible to move the authentication of a mainframe application user ID from RACF to another authorized function executing on the host system or to the work station local area network (LAN) environment.

Generating a PassTicket

A product or function that generates a PassTicket must use the RACF PassTicket generator algorithm. This algorithm requires specific information as input data and produces a PassTicket that substitutes for a specific end-user RACF password. RACF uses the PassTicket to authenticate the end-user for a specific application running on a specific system that uses RACF for identification and authentication.

There are two ways to generate a PassTicket using the algorithm:

- If the function using the secured signon capabilities is running on an MVS system, you can use the RACF secured signon service to generate the PassTicket. The algorithm is already incorporated into the service and allows RACF to generate a PassTicket on the host. An authorized program, such as one authorized by the authorized program facility (APF), can use the callable service to generate PassTickets. See “Using the Service to Generate a PassTicket” for more information.
- For any function that generates a PassTicket, you can create a program that incorporates the algorithm. See “Incorporating the PassTicket Generator Algorithm into Your Program” on page 294 for more information.

Using the Service to Generate a PassTicket

To allow RACF to authenticate a user with a PassTicket instead of a password, the non-RACF function performing the authentication calls the secured signon service to build a PassTicket.

The secured signon service:

- Is branch-entered by callers.
- Is *not* supported in cross-memory mode. Access register (AR) mode must use address space control (ASC).
- Is not supported in SRB mode.
- Requires that the caller be in key zero.

Before calling the secured signon service, the application must locate the address of the service. You can find this address from field RCVTPTGN in the RACF communications vector table (RCVT). The ICHPRCVT macro maps the RCVT and field CVTRAC points to it in the MVS communications vector table (CVT).

To be sure the label (RCVTPTGN) is resolved, if the system you are compiling on is an earlier level than MVS 5.1, you must make sure that the PTF associated with APAR OY65283 has been installed.

How the Secured Signon Service Works

The service:

- Uses standard linkage
- Uses the current system time, expressed in Greenwich Mean Time (GMT),¹ as input for the algorithm
- Returns the PassTicket in general purpose register 0 (the leftmost four characters) and general purpose register 1 (the rightmost four characters)
- Provides return codes
 - If a PassTicket is produced, register 15 contains a return code of 0
 - If a PassTicket is not produced, register 15 contains return code of 8

Notes:

1. Register 13 must point to a standard save area.
2. No additional recovery processing is provided by the secured signon service beyond what is already in effect within the invoking program.

Invoking the Secured Signon Service

Following is an example of a generalized programming technique you can use with assembler language to invoke a service. It is not intended to be syntactically correct.

```
L 15,RCVTPTGN  
CALL (15),(userid,appname)
```

where:

userid

Is the RACF user ID of the user the PassTicket authenticates. This field is a maximum of 9 bytes. The first byte contains the length of the non-blank portion of the *userid* field that follows. Bytes 2 through 9 contain the user ID and must be in uppercase and left-justified in the field.

appname

Is the application name that the secured signon function uses to locate the secured signon key used in the PassTicket generator algorithm. (See *z/OS Security Server RACF Security Administrator's Guide* for information on determining application names.) This field is a maximum of 9 bytes. The first byte is the length of the non-blank portion of the *appname* field that follows. Bytes 2 through 9 contain the application name and must be in uppercase and left-justified in the field.

When the secured signon service is invoked, only the *appname* (not the *userid* or *group*) is used to locate the secured signon key.

Incorporating the PassTicket Generator Algorithm into Your Program

To generate a PassTicket without using the RACF service, you need to incorporate the RACF PassTicket generator algorithm into your program.

The RACF PassTicket algorithm consists of two parts:

- The RACF PassTicket generator
- The RACF PassTicket time-coder

The time-coder is invoked from within the RACF PassTicket generator and returns its results to the generator.

1. GMT is also referred to as coordinated universal time (UTC).

The flowcharts in Figure 6 and Figure 7 on page 296 and the descriptions that follow show how to implement the RACF PassTicket generator algorithm.

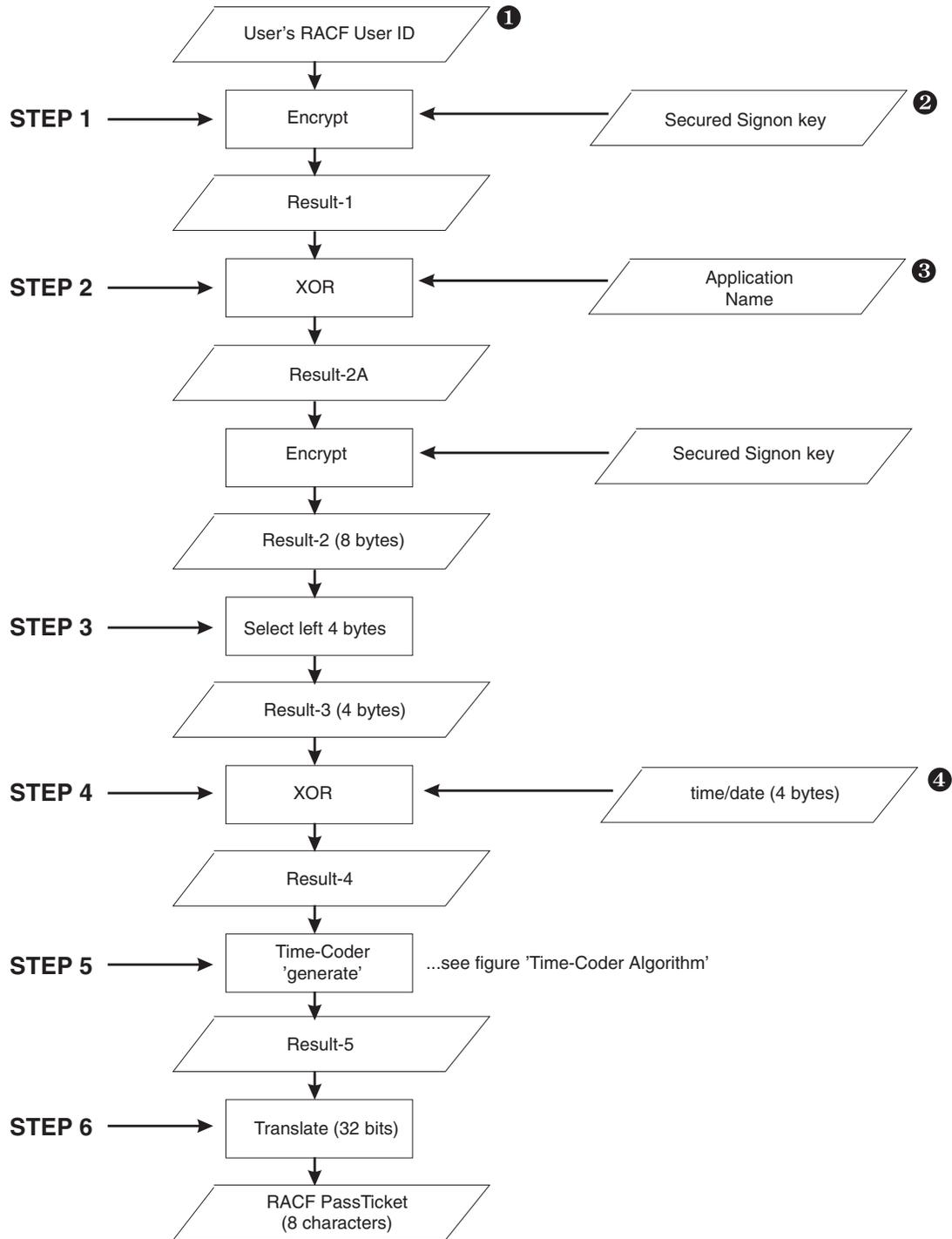


Figure 6. RACF PassTicket Generator for Secured Signon

PassTicket

...'Time-Coder Algorithm'

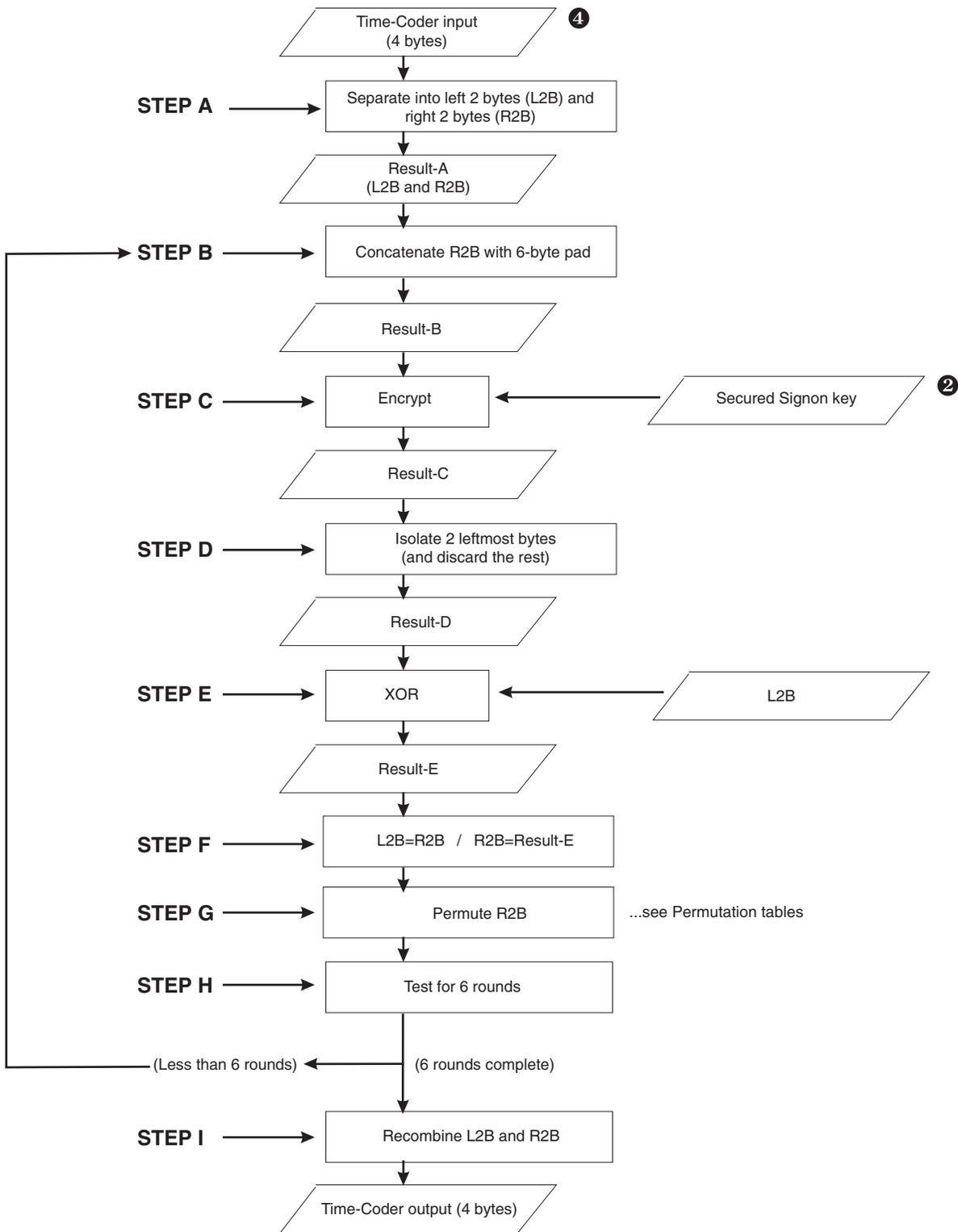


Figure 7. Algorithm for RACF PassTicket Time-Coder Used for Secured Signon

Input Data for the Algorithm

To successfully use the PassTicket, the target application using RACF to identify and authenticate a user ID needs to have specific information for processing according to the algorithm. As shown in Figure 7 on page 296, these are:

- A RACF host user ID
- The RACF secured signon application key
- The application name
- Time and date information

1 The RACF user ID

- Identifies the user ID on the system on which the target application runs
- Is represented in EBCDIC
- Is left-justified and padded with blanks on the right to a length of 8 bytes

2 The RACF secured signon application key

- Must match the key value used when defining the application to the PTKTDATA class to RACF
- Contains only the characters 0 through 9 and A through F

3 The application name as defined for a particular application. You can use it to associate a secured signon key with a particular host application. See *z/OS Security Server RACF Security Administrator's Guide* for information on determining application names.

The name:

- Is represented in EBCDIC
- Is left-justified and padded with blanks on the right to a length of 8 bytes

4 Time and date information and input data from the application that is providing the logon function. This information:

- Must be a 4-byte binary number
- Shows how many seconds have elapsed since January 1, 1970, at 0000 Greenwich Mean Time (GMT)

Several programming languages support a function for representing time in this way. In C language, for example, you can obtain the time in this way:

1. Declare the variable `ts` as `long`.
2. Invoke the function `time(&ts)`.

This produces the number of seconds that have elapsed since January 1, 1970 at 0000 GMT, expressed as an unsigned long integer.

Notes:

1. It is likely that the computer that authenticates the PassTicket is not the computer that generated it. To provide for differences in their internal clocks, the algorithm allows the generated time to be 10 minutes on either side of the TOD clock of the computer that is evaluating the PassTicket.
2. For RACF to properly evaluate PassTickets, the TOD clock must be properly set to GMT rather than local time.

How the Generator Algorithm Works

The RACF PassTicket generator algorithm uses the input information to create a PassTicket. By using cryptographic techniques, the algorithm ensures that each PassTicket is unpredictable.

PassTicket

The PassTicket is an 8-character alphanumeric string that can contain the characters A through Z and 0 through 9. The actual PassTicket depends on the input values.

The following steps describe this process (see Figure 6 on page 295 for a summary):

1. The RACF user ID **1** is encrypted using the RACF secured signon application key **2** as the encryption key to produce Result-1.

Note: All encryptions use the U.S. National Institute of Standards and Technology Data Encryption Standard (DES) algorithm. Only the DES algorithm encoding is involved. You cannot perform general encryption and decryption of data with this implementation.

2. Result-1 from the first encryption is XORed ² with the application name **3**. The application name must be 8 bytes of EBCDIC characters with trailing blanks. The result (Result-2A) is encrypted using the application key value **2** as the encryption key to produce Result-2.

Note: If you understand cryptographic techniques, you should recognize the flow (Steps 1 and 2) to be a common cryptographic architecture (CCA) standard message authentication code algorithm.

3. The left 4 bytes from Result-2 of the second encryption are selected as input to the next step. The rest are discarded.
4. The resulting 4 bytes (Result-3) are XORed with the time and date information **4**. The time and date is in the form of a 4-byte field that contains the number of seconds that have elapsed since January 1, 1970 at 0000 GMT in the form of a binary integer. (See “Input Data for the Algorithm” on page 297 for a complete description.)
5. The result (Result-4) of that procedure is passed to the time-coder routine. Refer to the diagram in Figure 7 on page 296 and to “How the Time-Coder Algorithm Works” to understand that process.
6. The result (Result-5) of the time-coder routine is translated, using a translation table described in “The Translation Table” on page 300, to an 8-character string called the PassTicket. It is used in the user’s host application signon request instead of the user’s regular RACF password.

How the Time-Coder Algorithm Works

The RACF PassTicket time-coder algorithm uses the result of Step 4 of the generator algorithm. It creates the time-coder information and passes it back to step 6 of that algorithm.

The following steps, which make up Step 5 of the generator algorithm, shown in Figure 7 on page 296 describe this process:

Step A Separate the 4-byte time-coder input (Result-4) into two portions, L2B (the left side), and R2B (the right side) to produce Result-A.

Step B

Note: If the system for which you are generating the PassTicket has RACF 1.9.2 or RACF 2.1 installed, make sure that APAR OW03024 is installed on that system. The PTF numbers are:

2. XOR is a Boolean function that processes two-bit strings of the same length, producing a third string of the same length as the output. In the output string, a bit is ON if the corresponding bit is ON for one of the input bit strings, but not both.

UW05405 For RACF 2.1.0
UW05406 For RACF 1.9.2

Concatenate R2B (the right 2 bytes from Result-A) with 6 bytes of padding bits to form Result-B. In the resulting 8-byte string, the 2 bytes of R2B occupy the leftmost 2 byte positions.

The padding bits consist of two separate 6 byte strings: PAD1 and PAD2. PAD1 is the left half and PAD2 is the right half of a 12 byte string consisting of the user ID (from Step 1 in “How the Generator Algorithm Works” on page 297) left justified and padded to the right with hexadecimal '55's. For example, if the user ID is “TOM”, PAD1 is 'E3D6D4555555' and PAD2 is '555555555555'. If the user ID is “IBMUSER”, PAD1 is 'C9C2D4E4D2C5' and PAD2 is 'D95555555555'. PAD1 is used for time coder loop rounds 1, 3, and 5. PAD2 is used for time coder loop rounds 2, 4, and 6.

- Step C** Result-B is encrypted using the RACF secured signon application key **2** as the encryption key to produce Result-C.
- Step D** The left 2 bytes from the Result-C are isolated and the rest of the value is discarded, producing Result-D.
- Step E** Result-D is XORed with L2B (from Result-A) to produce Result-E.
- Step F** The values of L2B and R2B are redefined:
1. L2B is set equal to R2B.
 2. R2B is set equal to Result-E.
- Step G** R2B is permuted ³ using the permutation tables in Figure 8 on page 300, where the table used reflects the number of the round. For example, for the first time through, R2B is permuted using table 1.
- Step H** This step counts the number of time-coder rounds that have been completed. If the value is less than 6, the time-coder returns to Step b for another round. If 6 rounds have been completed, processing continues with the next step.
- Step I** L2B (left 2 bytes) and R2B (right 2 bytes) are recombined into a 32-bit string. This completes the time-coder processing and produces Result-5. This result is passed back to the generator algorithm as input to Step 6 on page 298 for translation.

The Permutation Tables

A permutation table exists for each round of permutations that occurs during the time-coder process.

The six permutation tables work in the following manner:

- The upper of the two rows of numbers (O=>) represents the output positions, from left to right, of the 16 bits being permuted.
- The lower of the two rows (I=>) represents the input-bit position.

For example, using Permutation Table 1:

- Output-bit position 1 consists of the bit (on or off) in input-bit position 10.
- Output-bit position 2 consists of the bit in input-bit position 2.

3. To permute is to transform or change the order of members of a group.

PassTicket Character Position	Binary	Integer	Remainder	Translates to Character
1	010000	16	$16 \times 1/36 \Rightarrow 16$	Q
2	000111	7	$7 \times 1/36 \Rightarrow 7$	H
3	110010	50	$50 \times 1/36 \Rightarrow 14$	O
4	100100	36	$36 \times 1/36 \Rightarrow 0$	A
5	000111	7	$7 \times 1/36 \Rightarrow 7$	H
6	111111	63	$63 \times 1/36 \Rightarrow 27$	I
7	110111	55	$55 \times 1/36 \Rightarrow 19$	T
8	111001	57	$57 \times 1/36 \Rightarrow 21$	V

- Bits 31, 32, 1, 2, 3, and 4 (6 bits total) are translated to produce the PassTicket character in position 1.
The six bits (binary '010000' or decimal 16) are divided by decimal 36.
- The remainder (decimal 16) becomes the index into the translation table. The result is character 'Q'.
- Repeat the process for the rest of the bits.
 - Bits 3 through 8 are translated to PassTicket character 'H'.
 - Bits 7 through 12 are translated to PassTicket character 'O'.
 - Bits 11 through 16 are translated to PassTicket character 'A'.
 - Bits 15 through 20 are translated to PassTicket character 'H'.
 - Bits 19 through 24 are translated to PassTicket character 'I'.
 - Bits 23 through 28 are translated to PassTicket character 'T'.
 - Bits 27 through 32 are translated to PassTicket character 'V'.

The resulting PassTicket returned as output is QHOAH1TV.

Generating a Secured Signon Session Key

RACF can be invoked to generate a secured signon session key. A secured signon session key is a 64-bit value which can be used as a short-term session masking key for enhancing communication security between two network entities. The 64-bit value is a commercial data masking facility (CDMF) key which has an effective cryptographic strength of 40 bits. Because these keys are not highly secure, it is important that they be used only for communications of short duration.

Assume that a non-RACF z/OS or OS/390 application wants to communicate with a second party network entity. The application calls the secured signon session key generator service to create a secured signon session key based on a previously created PassTicket. The second party network entity uses the same algorithm and PassTicket to generate the same session key. The two network entities can now communicate securely without ever exchanging session keys.

Using the Service to Generate a Secured Signon Session Key

To allow RACF to create a secured signon session key, the non-RACF z/OS or OS/390 application calls the secured signon session key generator service.

The secured signon session key generator service:

- Is branch-entered by callers

PassTicket

- Is *not* supported in cross-memory mode
- Requires that the caller be in task mode, system key zero (0), and primary ASC mode

Before calling the secured signon session key generator service, the application must locate the address of the service. This address can be found in field RCVTSKGN in the RACF communications vector table, RCVT. The ICHPRCVT macro maps the RCVT and field CVTRAC points to it in the MVS communications vector table (CVT).

How the Secured Signon Session Key Generator Service Works

The service:

- Uses standard linkage
- Uses the PassTicket as input for the algorithm
- Returns the session key in general purpose register 0 (4 bytes) and general purpose register 1 (4 bytes)
- Provides return codes

Notes:

1. The secured signon session key generator service uses either the current task level or address space level ACEE unless an ACEE address is passed on the input parameter list.

If an application is using a RACF PassTicket to authenticate users and wants to derive a session key for securing application-to-user communication, the application must establish a task level ACEE for its client or point to the client's ACEE. The following calls must be made **in this sequence**:

- a. A RACROUTE REQUEST=VERIFY,ENVIR=CREATE request to authenticate and create a task level ACEE for the application's client. (This request can be omitted if the client's ACEE was previously created by a RACROUTE REQUEST=VERIFY.)
 - b. Construct a secured signon session key generator parameter list and branch to the address pointed to by RCVTSKGN.
2. Register 13 points to a standard savearea.
 3. No additional recovery processing is provided by the secured signon session key generator service beyond what is already in effect for the invoking program.

Invoking the Secured Signon Session Key Generator Service

Following is an example of a generalized programming technique you can use with assembler language to invoke this service. It is not intended to be syntactically correct.

```
LA 1,MY_APPL_PLIST
L 15,RCVTSKGN
CALL (15),(1)
```

Register 1 points to MY_APPL_PLIST which contains:

Displacement	Description
+0	A pointer to the RACF PassTicket used for user authentication
+4	A pointer to a one-byte length field followed by up to 8 characters which is the APPLID
+8	A pointer to the address of the user ID's ACEE that was created during PassTicket evaluation. If the address is zero, the task level ACEE (TCBSENV) is used if it exists. If not, the address space level ACEE (ASXBSENV) is used.

Return Codes from the Secured Signon Session Key Generator Service

The secured signon session key generator service produces the following return codes in register 15:

Note: The values shown are in hexadecimal.

Return Code	Description
0	Successful completion. The resulting session key is contained in general purpose registers 0 and 1.
4	Incorrect PassTicket
8	No PTKTDATA profile found for the application
C	No task or address space ACEE found, and the ACEE pointer was not specified on the input parameter list.
10	Caller is not authorized
14	The RACF PTKTDATA class is not active
18	Error in the session key generator process

Incorporating the Secured Signon Session Key Generator Algorithm into Your Program

To generate a secured signon session key without using the secured signon session key generator service, you need to incorporate the secured signon session key generator algorithm into your program.

In order to ensure identical session key generation on both platforms, the following steps must be implemented by both the non-RACF application and the second party network entity.

The secured signon session key generator algorithm consists of two parts:

- Secured signon session key generation logic
- CDMF key-weakening logic

The flowcharts in Figure 10 on page 304 and Figure 11 on page 305 and the descriptions that follow show how to implement the secured signon session key generator algorithm.

Secured Signon Session Key Generation Logic

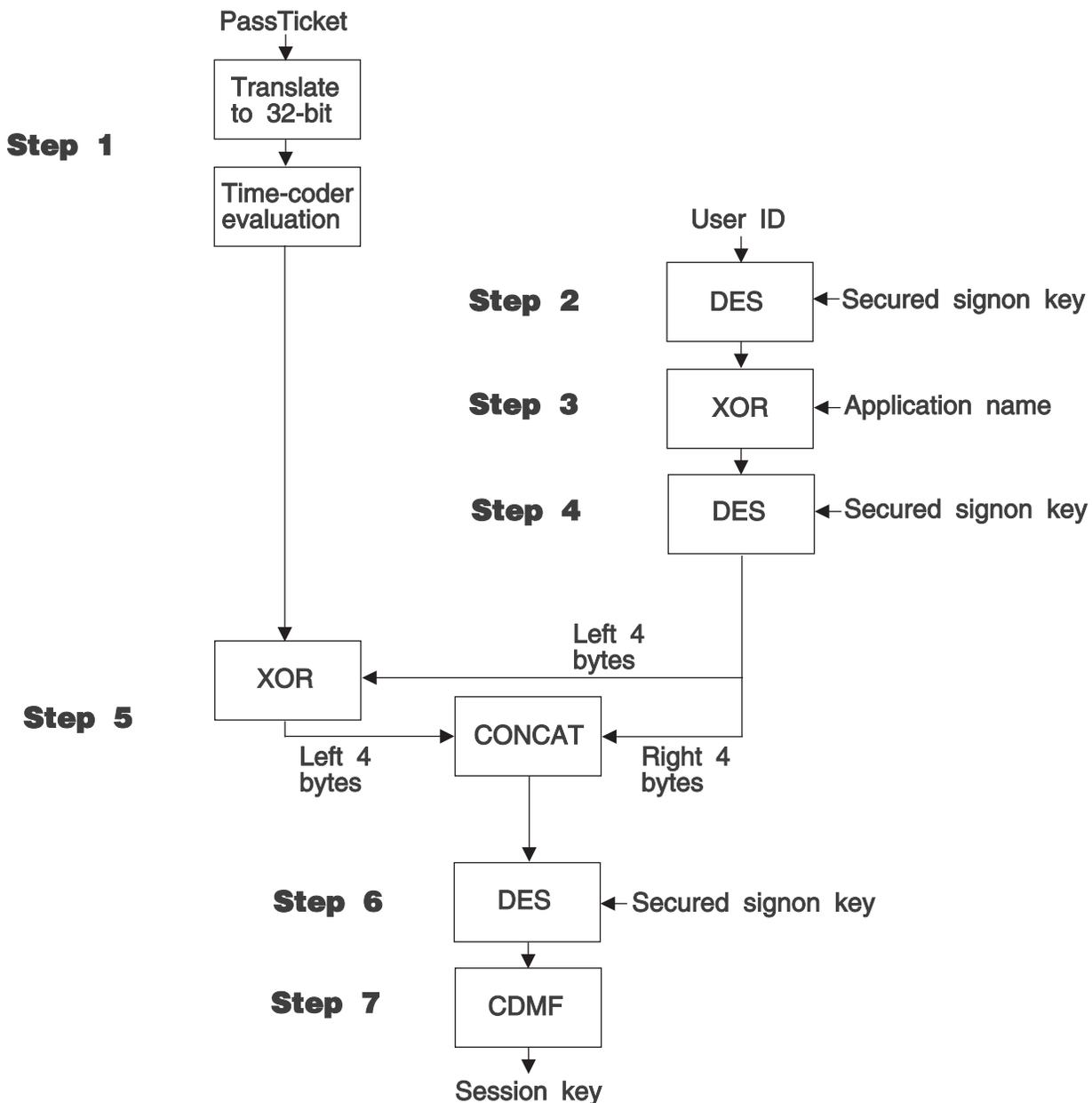


Figure 10. Secured Signon Session Key Generation Logic

The secured signon session key generation logic is:

1. The PassTicket used to establish the session is time-coder evaluated to extract the time stamp.
This is the reverse process of steps 5 and 6 as described in “Incorporating the PassTicket Generator Algorithm into Your Program” on page 294. If the time stamp used to generate the PassTicket is already known, this step can be skipped.
2. The input user ID is DES-encrypted with the secured signon key shared with the second party network entity.

Note: Steps 2 through 4 of this secured signon session key generation logic are the same as steps 1 and 2 of "Incorporating the PassTicket Generator Algorithm into Your Program" on page 294.

- 3. The result of step 2 is XORed with the non-RACF application name.
- 4. The result of step 3 is again DES-encrypted with the secured signon key.
- 5. The left 4 bytes of the result of step 4 are XORed with the left 4 bytes of the time stamp (result of step 1) and then concatenated with the right 4 bytes of the result of step 4.
- 6. The result of step 5 is DES-encrypted with the secured signon key to produce a strong session key.
- 7. The result of step 6 is weakened using CDMF to produce the final secured signon session key.

CDMF Key-Weakening Logic

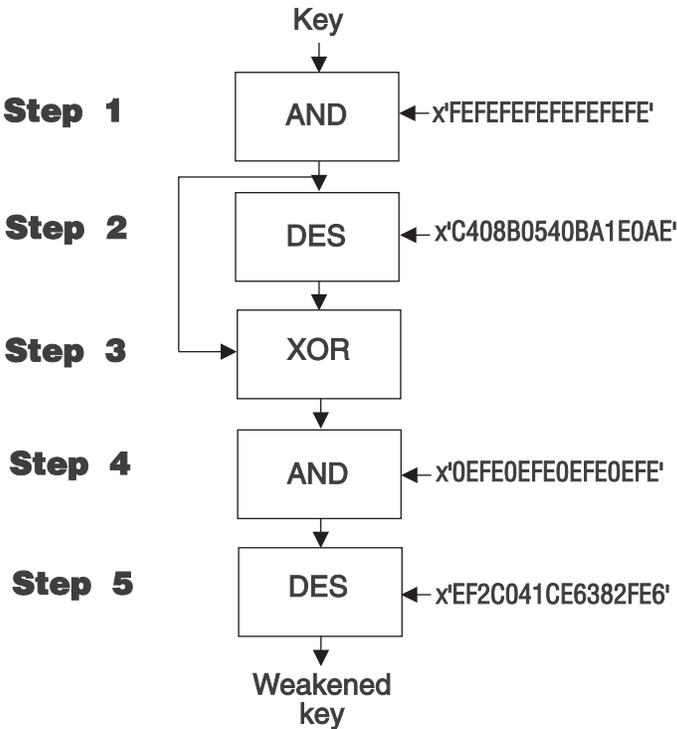


Figure 11. CDMF Key-Weakening Logic

The CDMF key-weakening logic is:

- 1. The parity bits of the key are zeroed by ANDing it with the string X'FEFEFEFEFEFEFEFE'.
- 2. The result of step 1 is DES-encrypted with the key X'C408B0540BA1E0AE'.
- 3. The result of step 2 is XORed with the result of step 1.
- 4. The result of step 3 is ANDed with the string X'0EFE0EFE0EFE0EFE'.
- 5. The result of step 4 is DES-encrypted with the key X'EF2C041CE6382FE6' to produce the weakened key.

PassTicket

Chapter 12. The RACF Environment Service

RACF provides the environment service, IRRENS00, that is located through the RCVT. An RCVT flag, RCVTENVS, indicates that the service is present. When the flag is on, RCVTENVP contains the address of IRRENS00.

Note: Note: This service is to be used only by z/OS UNIX System Services and is not intended for customer use. Information on this service is provided here to assist security vendors in understanding IRRENS00 operations.

Function

Keep-Controlled

Verifies that the environment is currently controlled, and if so sets flags indicating that it must remain controlled. It also saves a message supplied by the caller indicating the reason it must remain controlled. It keeps separate flags for z/OS UNIX requests and RACF requests.

Mark-Uncontrolled

Determines whether the environment must remain controlled by inspecting the keep-controlled indicators and (if necessary) the PADS data set list from the ACEE and the CDEs for modules in the address space, and if not, marks it uncontrolled and also marks any existing TCBS and CDEs as uncontrolled. However, if a keep-controlled request is outstanding, mark-uncontrolled returns an error code and either issue (WTO) any saved messages from a previous keep-controlled request or generates messages to indicate why RACF needed the environment kept controlled. For a successful request, mark-uncontrolled also saves a caller-provided message indicating why the environment became uncontrolled, which it issues on subsequent keep-controlled requests if necessary.

Reset Keep-Controlled

Resets the keep-controlled indicators and remove any saved messages relating to previous keep-controlled requests. It is intended only for use by z/OS UNIX when z/OS UNIX determines that the environment no longer needs to be kept controlled.

Requirements

1. Authorization: Both supervisor state and key 0.
2. Dispatchable Unit Mode: Task
3. Cross-Memory Mode: PASN=HASN=SASN
4. AMODE: 31
5. RMODE: Any
6. ASC Mode: Primary
7. Recovery Mode: Estae (caller cannot have an FRR)
8. Serialization: This service obtains Local lock and uses compare and swap for serialization
9. Control Parameters: The parameter list and all parameters must be in the primary address space

RACF Authorization

None

Register Usage

Registers on input:

1 Parameter list address
13 Savearea address
14 Return address
15 Address of IRRENS00 from RCVTENVP

Registers on return:

0 Reason code
1–12 Unknown
13 Savearea address
14 Return address
15 Return code

Format

```

*      .
*      .
*      .
      L      Rx,CVTPTR
      USING CVT,Rx
      L      Rx,CVTRAC
      USING RCVT,Rx
      TM     RCVTMFL1,RCVTENVS    Test for service availability
      BZ     not_available        bypass call if not available
      L      R15,RCVTENVP        Get service address
      LA     R1,parms            Get parameter list area
      L      R13,save_area        Must provide a save area
      BALR  R14,R15              Call the service
*      .or CALL (15),(work_area,function_code,function_flags,return_code,
*      .                                reason_code,message_block)
      DROP  Rx
      ...
parms DS      0F
      DC     A(work_area)
      DC     A(function_code)
      DC     A(function_flag)
      DC     A(return_code)
      DC     A(reason_code)
      DC     A(message_block)
      ...
work_area DS   0D,XL2048
function_code DS  F
function_flags DS  F
return_code DS  F
reason_code DS  F
message_block DS  0F
message_text DS  F'length',CL(length)'text'
*      .

```

Parameters

work_area 2048 bytes, doubleword aligned. Used as internal storage by IRRENS00.

function_code
Fullword; input:

X'00000000' Keep-Controlled
X'00000001' Mark-Uncontrolled
X'00000002' Reset Keep-Controlled
X'00000003' Mark HFS

function_flag Fullword; input:

For Mark_Uncontrolled:

X'00000000' IRRENS00 should issue WTO on failure.
X'00000001' IRRENS00 should not issue WTO.
X'80000000' Request by z/OS UNIX for HFS control.

For Keep-Controlled:

X'80000000' Request by z/OS UNIX.
X'40000000' Request by RACF.

Note: One, and only one, of the above flags must be on.

X'00000000' IRRENS00 should issue WTO on failure.

X'00000001' IRRENS00 should not issue WTO.

X'00000002' Only UNIX mark-uncontrolled should be checked before marking keep-controlled.

X'00000004' Indicates that RACF should determine whether ENHANCED program security is in effect for this job, and if so RACF should determine whether execution environment was established by a MAIN program or not. If not, RACF either fails the request or sets a warning with return and reason codes. Additionally, RACF should issue appropriate messages, including those saved from a prior call to IRRENS00.

For Reset Keep-Controlled:

X'80000000' Reset the UNIX keep-controlled flag and clear the related saved message.

X'40000000' Reset the RACF keep-controlled flag and clear the related saved message.

X'20000000' Clear any message saved for a previous mark-uncontrolled function, and reset the UNIX mark-uncontrolled flag.

Note: At least one of the above flags must be on.

For Mark HFS:

X'80000000'
 Indicates a call from z/OS UNIX System Services.

Note: The above flag must be on.

return_code Fullword; output. See **Note** below.

reason_code Fullword; output. See **Note** below.

message_block
 Fullword length of text, followed by the text; input.

Note: The fullword must be non-zero and message text must be provided for the keep-controlled and mark-uncontrolled functions. The maximum message text length allowed is 250. The fullword must be 0 for the reset keep-controlled function.

IRRENS00

For keep-controlled and mark-uncontrolled, the caller will use this parameter to provide a message indicating the reason for the request. The first character of the message must not be a blank. The message must begin with a message ID (such as BPXnnnl or ICHnnnl), followed by a blank. When the message is displayed, a maximum of 71 characters will appear on each line of the display. If a blank does not appear in column 71 or column 72, the message text will be split to a new line at the preceding blank. The caller providing the message must document it in their manuals. Message text must be upper case, contain only alphanumeric and national characters, and should be NLS compliant.

A copy of the message provided by the caller will be saved and IRRENS00 will issue this message, among others, during failing keep-controlled requests or failing mark-uncontrolled requests. The messages will be issued with descriptor code 6 and routing codes 9 and 11, directing them to the security console and the programmer.

The caller is not responsible for deleting the saved copy of the messages. Saved messages will be cleared and their storage released by the Reset Keep-Controlled function when the corresponding keep-controlled indicator is reset. IRRENS00 is responsible for ensuring the storage used to contain the saved messages is released appropriately when no longer needed.

Return and Reason Codes

IRRENS00 returns the following return and reason codes:

Return Code	Meaning
--------------------	----------------

0	Function successful
---	---------------------

	Reason Code
--	--------------------

	0
--	---

	20	Indicates that a caller requested a MAIN check through function flag X'00000004', that enhanced program security is in effect in warning mode for the current job, and the current execution environment was not established by a MAIN program.
--	----	---

4	Function not processed; parameter error
---	---

	Reason Code	Meaning
--	--------------------	----------------

	4	Incorrect function code
--	---	-------------------------

	8	Incorrect function flags for specified function code
--	---	--

	C	Incorrect message block for specified function code
--	---	---

8	Function failed
---	-----------------

	Reason Code	Meaning
--	--------------------	----------------

	4	Cannot mark keep-controlled for UNIX; already uncontrolled
--	---	--

	8	Cannot mark keep-controlled for RACF; already uncontrolled
--	---	--

	C	Cannot mark uncontrolled; marked keep-controlled for z/OS UNIX
--	---	--

	10	Cannot mark uncontrolled; marked keep-controlled for RACF
--	----	---

	20	Indicates that a caller requested a MAIN check through function flag X'00000004', that enhanced
--	----	---

program security is in effect in failure mode for the current job, and the current execution environment was not established by a MAIN program.

Note: Keep-controlled can only fail due to the environment already being marked uncontrolled. Likewise, mark-uncontrolled can only fail because of a previous keep-controlled request. For a mark uncontrolled request, the UNIX keep-controlled request will be checked first, and if on, return code 8 and reason code C will be returned, without additional checking for RACF keep-controlled.

C Internal error

Reason Code

0

Usage Notes

1. Callers (including z/OS UNIX) can use the IRRENS00 service after checking that RCVTENVS='1'B. The address for IRRENS00 is obtained from RCVTENVP.
2. To ensure that a message is saved, the mark-uncontrolled function of IRRENS00 should be used rather than setting TCBNCTL directly.
3. Only IRRENS00 will set, check or reset the keep-controlled indicators. Resetting can occur when the reset function is requested, or at other times if IRRENS00 determines the environment no longer needs to be kept controlled. For example, during a mark-uncontrolled request IRRENS00 may find RACF's keep-controlled indicator set, but find no open program-accessed data sets and no execute-controlled modules present. In this case, it will turn off RACF's keep-controlled indicator, and if the z/OS UNIX indicator is off, it will honor the request.
4. The UNIX mark-uncontrolled indicator is kept internally by the security product, and is set in addition to TCBNCTL. Defining BPX.DAEMON.HFSCTL in the FACILITY class requests z/OS UNIX enforce HFS control only. This option is appropriate when the loading of uncontrolled files must be restricted to protect against changes made by superusers, but the loading of uncontrolled programs from MVS libraries does not introduce any security concerns.

With HFS control in effect, z/OS UNIX passes the UNIX mark-uncontrolled indicator to IRRENS00 when an uncontrolled file is loaded from the HFS. The message passed with the first UNIX mark-uncontrolled request will always be saved.

With HFS control in effect, z/OS UNIX passes the check UNIX mark-uncontrolled indicator to IRRENS00 on a keep-controlled request indicating that the request to keep-controlled should only fail if UNIX marked the environment uncontrolled.

The UNIX mark-uncontrolled indicator is reset when the messages saved for previous mark-uncontrolled requests are cleared by the reset function.

Related Services

None

Appendix A. ICHEINTY, ICHETEST, and ICHEACTN Macros

The ICHEINTY, ICHETEST, ICHEACTN product macros are described in this appendix, rather than in the body of the book, because of their complexity and the cautions required in their use.

Recommendations:

- You should use the RACROUTE REQUEST=EXTRACT instead for the cases where it can be used. However, only the RACF command processors completely validate the data entering the database, so it is better to use RACF commands than either ICHEINTY or RACROUTE REQUEST=EXTRACT when updating the database. For more information on RACROUTE REQUEST=EXTRACT, see *z/OS Security Server RACROUTE Macro Reference*.
- In general, you should use the RACF commands to create RACF resource profiles. If you use ICHEINTY instead, you should create profiles which are supported by the command processors. For instance, ICHEINTY allows you to create a fully-qualified generic profile in a general resource class and a data set profile containing characters that are not valid, but those profiles are not supported by the RACF command processors.

You can use the ICHEINTY, ICHETEST, and ICHEACTN macros to locate (retrieve) and update the various profiles on the RACF database.

ICHEINTY Locates or updates the profile.

ICHETEST Tests for user-specified conditions on selected fields in the profile.

ICHEACTN Retrieves or alters specified fields within the retrieved profile.

If you plan on using these macros, you should exercise caution because they:

- Perform only limited parameter validation. The module issuing these macros must be authorized (supervisor state, system key, or APF-authorized).
- Do not pass control to any exit routines except indirectly. If FLDACC=YES was specified on the ICHEINTY macro, the RACROUTE REQUEST=AUTH exits will be given control during field access checking.
- Do not do any logging except indirectly. Logging can occur during field access checking if the RACROUTE REQUEST=AUTH request exit requests it.
- Do not complete data consistency checking. For example,
 1. They do not ensure that all fields in a profile will have the data expected by subsequent RACF processing.
 2. They do not ensure that related profiles are updated in a consistent manner. For example, a group profile must point to its superior group profile and the superior group must point to the subgroup profile. The command processors would ensure this, but these macros do not.

Note: You should thoroughly familiarize yourself with the template information contained in Appendix D, "RACF database templates" before you read this section.

These macros can be used by callers in either 31- or 24-bit addressing mode. The parameter lists can be located above 16MB if the caller is in 31-bit mode.

Application programs must be structured such that a task requesting RACF services does not do so while other I/O initiated by the task is outstanding. If such I/O is

required, the task should either wait for the other I/O to complete before requesting RACF services, or the other I/O should be initiated under a separate task. This is necessary to assure proper processing in recovery situations.

ICHEINTY Macro

The ICHEINTY macro provides a direct interface to the RACF database through the RACF manager. Its function is to locate and/or update a profile in the RACF database.

You can use the ICHEINTY macro with the ICHETEST and ICHEACTN macros to test and conditionally update fields in RACF profiles.

The ICHEINTY macro must be issued from a task running in non-cross-memory mode with no locks held. The issuing task must be authorized (APF-authorized, in system key 0-7, or running in supervisor state).

You may reference only one segment with each ICHEINTY call; however, you may access more than one field in a segment using a single call. If you need to retrieve or update more than one segment, issue a separate ICHEINTY for each segment.

When activated, automatic direction of application update propagates ICHEINTY ADD, ALTER, DELETE, DELETEA, and RENAME updates to selected remote nodes. Only ICHEINTY requests with return code 0 are propagated.

The format of the ICHEINTY macro definition is:

```
[label] ICHEINTY [operation]
                [,TYPE='GRP'|'USR'|'CON'|'DS'|'GEN']
                [,ENTRY=entry-address]
                [,ENTRYX=extended-entry address]
                [,CLASS=class-address]
                [,FLDACC=NO|YES]
                [,RELEASE=number|(,CHECK)|(number,CHECK)]
                [,RUN=YES|NO]
                [,ACEE=acee address]
                [,WKSP=subpool number]
                [,CHAIN=parm-list address]
                [,DATAMAP=OLD|NEW]
                [,SEGMENT='segment name']
                [,VOLUME=volume-address]
                [,ACTIONS=(action-address,...)]
                [,TESTS=(test-addr[, [AND], test-addr]...)]
                [,WKAREA=workarea-address]
                [,NEWNAME=newname-address]
                [,NEWNAMX=extended-newname-address]
                [,RBA=rba-address]
                [,FLDEF=fldef-address]
                [,OPTIONS=( [NOPRO|TESTM|TESTC|ACTION|
                            NOEXEC|FLDEF],...)]
                [,SMC=YES|NO]
                [,GENERIC=NO|YES|UNCOND]
                [,DATEFMT=YYDDDF|YYYYDDDF]
                [,MF=I|L|(E,address)]
```

operation

specifies the operation that RACF is to perform on the specified profile. The valid operation values are ADD, ALTER, ALTERI, DELETE, DELETEA, FLDEF, LOCATE, NEXT, NEXTC, and RENAME. This operand is positional and is required if you specify MF=I or MF=L.

Some operations are based on assumptions. If a requested operation violates an assumption, the operation fails.

ADD

defines entities to RACF by adding profiles to the RACF database. ADD processing:

- Creates a profile for the new entry with fields containing null values. (See “Using ICHEACTN to Alter Data When the ICHEINTY Has DATAMAP=NEW” on page 339 and “Using ICHEACTN to Alter Data When ICHEINTY Has DATAMAP=OLD” on page 342.)
- Alters field values as specified by associated ICHEACTN macro instructions.
- Allocates space for the profile on the RACF database and writes the profile.
- Creates an index entry for the profile. The index entry points to the new profile.

Some considerations regarding ADD are:

- ADD processing assumes that the profile does not already exist. If the profile already exists (the index contains the profile name), any of the following conditions causes a return code of 8 (X'08'):
 - TYPE is not 'DS'
 - TYPE is 'DS' and duplicate data set name creation has been prohibited via ICHSECOP.
 - TYPE is 'DS' and one of the existing profiles for the entity name contains in its volume list the volume specified by the VOLUME keyword.
- For TYPE='DS', ICHEINTY sets a return code of 60 (X'3C') if VOLUME is not specified and there are multiple profiles for the entity name.
- For TYPE='USR', when Automatic Direction of Application Updates and Automatic Password Direction are active; a single ICHEINTY with ACTIONS= that specifies both add user and password information results in the propagation of 2 requests to the target node, one by Automatic Direction of Application Updates, the other by Automatic Password Direction. At the target node, these two requests execute using different userids and can execute concurrently, this makes the results of the ICHEINTY unpredictable at the target node. The unpredictable results occur for the propagation of any combination of ICHEINTYs (a program with a single ICHEINTY, or multiple ICHEINTYs within the same or different programs) that define/ add a user and specify password information for that user.

Recommendation: You should use an ADDUSER command or the R-ADMIN function from an application program to define a RACF user under these conditions.

- For TYPE='GEN', you can add the same entity name to any number of different classes. If the class is TAPEVOL, ICHEINTY sets a return code of 60 (X'3C') if a VOLUME is specified but is not an existing TAPEVOL. ICHEINTY creates a profile for a TAPEVOL only when VOLUME is not specified; otherwise, it updates an existing profile. The macro creates an index entry in either case. The result of this special TAPEVOL processing is that RACF maintains only one profile for a multivolume tape. You can refer to that profile by specifying any of the volumes it protects.
- You must supply all the information required by RACF for subsequent processing: for example, owner, creation date.
- In general, you should use the RACF command processors to create RACF resource profiles. If you use ICHEINTY instead, you should create profiles which are supported by the command processors. For instance, ICHEINTY

ICHEINTY Macro

allows you to create a fully-qualified generic profile in a general resource class and a data set profile containing characters that are not valid, but those profiles are not supported by the RACF command processors.

ALTER

alters field values in an existing profile on the RACF database. ALTER processing:

- Locates the profile on the RACF database.
- Performs the tests that the ICHETEST macros specify, if any macros are present. The TESTS operand on the ICHEINTY macro names the tests to be performed.
- Alters field values as specified by associated ICHEACTN macro instructions.
- Writes the profile back to the primary and backup (if active) RACF databases.

Some considerations regarding ALTER are:

- If the profile is too large to be rewritten to the same location in the RACF database, RACF allocates new space, writes the profile to the new location, and updates the index entry for the profile to point to the new location.
- Do not use ICHEINTY to ALTER (or ALTERI) repeat group count fields. These fields are updated automatically whenever a repeat group changes its size. Repeat group count fields may be read.

ALTERI

is similar to the ALTER operation with the following exceptions:

- Fields are updated in place. ICHEINTY sets a return code of 68 (X'44') and fails the operation if the altered profile has a length which differs from that of the original profile.
- The update to the field occurs with only a shared lock on the RACF database. Therefore, other ALTERI, LOCATE, NEXT, or NEXTC requests can take place simultaneously.
- You can specify the RBA of the level one index block, containing the pointer to the profile to be altered. This improves processing efficiency.
- ALTERI processing writes the profile back to the primary RACF database only; it does not write to the backup, unless you have otherwise specified in the data set name table (ICHRDSNT). RACF uses ALTERI to update statistical information in profiles. ALTERI should only be used with fields that are marked in the template as statistical. For more information on the RACF database templates, see the Appendix D, "RACF database templates" on page 391.

DELETE

deletes a profile from the RACF database. DELETE processing:

- Deletes the index entry for the entity.
- Frees space used for the profile on the RACF database.

Some considerations regarding DELETE are:

- You cannot specify the ACTIONS operand with the DELETE operation.
- For TYPE='DS', ICHEINTY sets a return code of 60 (X'3C') if you specified VOLUME and a profile containing the specified volume in its VOLSER list was not found. ICHEINTY sets a return code of 56 (X'38') if you do not specify VOLUME and there are multiple profiles for the entity name.

- ICHEINTY deletes the profile for a TAPEVOL only when the volume being deleted is the last in its set. Otherwise, the macro deletes the index entry and removes the volume from the VOLSER list.

DELETEA

Deletes all the members of a TAPEVOL set from the RACF database. It is similar to the DELETE operation with the following exception:

- If you specify 'TYPE=GEN' and the class is TAPEVOL, ICHEINTY deletes the profile along with the index entry for each volume in the set.

FLDEF

Builds the area that the FLDEF operand uses. The area contains control information and the list generated by the TESTS and ACTIONS operands.

Some assumptions and considerations regarding FLDEF are:

- FLDEF creates a separate area for ICHEACTN and ICHETEST pointers, which can be referenced from one or more ICHEINTY macros.
- You can maintain the field definition area with the MF=E form of ICHEINTY FLDEF.
- When referencing the field definition area from a remote ICHEINTY, specify FLDEF=field-definition-area, and do **not** specify any of the ACTION, FLDEF, TESTC, and TESTM options on the OPTIONS keyword.

LOCATE

Retrieves zero or more fields from an existing RACF profile in the RACF data set. LOCATE processing:

- Locates the profile in the RACF database.
- Performs the tests that the ICHETEST macros specify, if any macros are present. The TESTS operand on the ICHEINTY macro names the tests to be performed.
- Retrieves field values as specified by associated ICHEACTN macro instructions into the caller-specified work area.

Some assumptions and considerations regarding LOCATE are:

- ICHEINTY sets a return code of 44 (X'2C') if the values being returned are too large for the work area provided and you did not specify the WKSP operand, which would have provided you with an additional work area.
- For TYPE='DS', ICHEINTY set a return code of 60 (X'3C') if you specify VOLUME and one or more profiles were found for the data set name but none contained the specified volume name in its VOLSER list. ICHEINTY sets a return code of 56 (X'38') if you do not specify VOLUME and there are multiple profiles for the entity name.
- ICHEINTY sets a return code of 52 (X'34') if an ICHETEST macro specified by the TESTS operand failed. The LOCATE operation terminates at this point.

NEXT

Retrieves zero or more fields from the profile whose name follows the name specified by the ENTRY or ENTRYX operand. The NEXT operation updates the area pointed to by the ENTRY or ENTRYX operand with the name of the profile just completed. NEXT processing:

- Locates the profile of the first entity of the specified type that follows the specified entity located in the RACF database.

ICHEINTY Macro

- Performs the tests that the ICHETEST macros specify, if any macros are present. The TESTS operand on the ICHEINTY macro names the tests to be performed.
- Retrieves field values as specified by associated ICHEACTN macro instructions into the caller specified work area.

Some considerations regarding NEXT are:

- If the entity retrieved has the same name as the entity that follows it in the RACF database, ICHEINTY sets the duplicate data set name count. The count becomes 2 if it was zero on entry; otherwise, the count increases by one. The count is zero if the entity is not a duplicate of the one that follows it.
- ICHEINTY sets a return code of 44 (X'2C') if the values being returned do not fit into the provided work area, unless you specified WKSP which would provide you with an additional work area.
- For qualified types (data set, general, and connect), the located entity must have the same high-level qualifier as the specified entity. Otherwise, the macro sets a return code of 12 (X'0C').
- For data set profiles, the qualifier includes the first period in the name.
- For TYPE='DS', if the duplicate data set name count in the work area is not zero, ICHEINTY locates the specified data set name. (That is, if the duplicate data set count equals N, then the macro locates the Nth occurrence of the specified name. If there are less than N occurrences of the specified name, the same process occurs as when the duplicate data set count is zero; ICHEINTY locates the profile of the first entity of the specified type that follows the specified entity in the RACF data set.) If you want to locate the first DATASET profile with a name greater than or equal to the name specified by ENTRY= or ENTRYX, you can do so by setting the duplicate data set name count to one.
- If an ICHETEST macro specified in the TESTS operand failed, ICHEINTY sets a return code of 52 (X'34') and the NEXT operation terminates.
- If you specify a segment other than BASE on this ICHEINTY, or on any ICHEINTY in a chain, the RACF manager skips any profiles that do not contain an occurrence of the segment. Normal processing (TESTS on ICHEINTY, ICHEACTN) will resume with the next profile containing the segment. This simplifies the process of finding users who are defined to TSO, for example.

NEXTC

is similar to the NEXT operation with the following exception:

- For qualified types (data set, general, and connect), ICHEINTY does not make the high-level qualifier check. For unqualified types (group and user), NEXTC processing is identical to NEXT processing. The qualifier for a general profile is the 8-character class name.

Note: You should not use NEXTC with general resource classes, as it might have unpredictable results. When you reach the end of the profiles for the class you specified with the CLASS keyword, ICHEINTY retrieves the first profile for the next general resource class that has profiles. However, you have no way of determining what class that profile belongs to, and in some cases you might not even know that ICHEINTY has switched to a new class.

RENAME

renames a data set, SFS file, or SFS directory entry in the RACF database.

You must specify the NEWNAME or NEWNAMX operand.

When renaming resources in the FILE and DIRECTORY class, use ENTRYX and NEWNAMX.

TYPE= 'GRP'I'USR'I'CON'I'DS'I'GEN'

Specifies the type of the entry as GROUP ('GRP'), USER ('USR'), CONNECT ('CON'), DATASET ('DS'), or general resource ('GEN').

The final parameter list the SVC uses as a request to the RACF manager must include a value for TYPE.

ENTRY= entry-address

Specifies the address of a 1-byte entry name length field followed by the entry name. The NEXT and NEXTC operations update this field. When using NEXT or NEXTC you should initialize the field in this way. To initialize the entry field, point to a field that has a length of 1 and a field of X'00'. The area pointed to must allow for 255 bytes of data to be returned.

The final parameter list the SVC uses as a request to the RACF manager must include a value for ENTRY or ENTRYX.

ENTRYX= extended-entry-address

Specifies the extended entry name field for long name support. You must specify the address of *two* 2-byte fields, followed by the entry name.

- The first 2-byte field specifies a buffer length which can be from 0 to 255 bytes. This length field only refers to the length of the buffer that contains the entity name; it does not include the length of either length field.
- The second 2-byte field specifies the actual length of the entity name. This length field includes only the length of the actual name without any trailing blanks; it does not include the length of either length field.

As with ENTRY, the NEXT and NEXTC operations update this field. The area pointed to must allow for a name which is of maximum entry length. ENTRY and ENTRYX are mutually exclusive keywords.

Recommendation: You should use the ENTRYX keyword because by allowing you to code to the specific amount of space that you need, you will save storage.

The final parameter list the SVC uses as a request to the RACF manager must include a value for ENTRY or ENTRYX. To use the ENTRYX keyword, you must specify RELEASE=1.9.

CLASS= class-address

Specifies the address of an 8-character class name (left-justified and blank-padded, if necessary.) The class name is required when TYPE='GEN' and is ignored for all other types.

FLDACC =NOIYES

Specifies the presence or absence of field level access checking. If you specify FLDACC=YES, the RACF database manager checks to see that the user running your program has the authority to retrieve or modify the fields that have been specified in the ICHETEST and ICHEACTN macros associated with the current ICHEINTY macro.

Note: For field level access checking to occur, you must specify RELEASE=1.8 or later when you code the ICHEINTY and associated ICHETEST and/or ICHEACTN macros. RACF will bypass field access checking for any ICHETEST or ICHEACTN macro for which RELEASE=1.8 or later has

ICHEINTY Macro

not been specified. In addition, before your program executes, the security administrator must activate the FIELD class and process the FIELD class using SETROPTS RACLIST. If you code FLDACC=YES and the field class is not active and has not been processed using SETROPTS RACLIST, the request will fail with a return code of 60.

A further note: in addition, the security administrator must issue the RDEFINE and PERMIT commands to designate those users who will have the authority to access the fields designated in the ICHETEST and ICHEACTN macros.

If you specify FLDACC=NO or omit the parameter, the manager does not perform field level access checking.

RELEASE=number

RELEASE=(,CHECK)

RELEASE=(number,CHECK)

Specifies the release number. The release numbers you can specify with the ICHEINTY macro are 7707, 7706, 7705, 7703, 2608, 2.6, 2.4, 2.3, 2.2, 2.1, 1.9.2, 1.9, 1.8.1, 1.8, or 1.7.

When you specify 1.8 or later, the RACF manager returns data using the new 1.8 user work area format (documented under the sections entitled “Using ICHEACTN to Retrieve Data When the ICHEINTY Has DATAMAP=NEW” and “Using ICHEACTN to Retrieve Data When the ICHEINTY Has DATAMAP=OLD” in this chapter). In effect, DATAMAP defaults to DATAMAP=NEW if you specify RELEASE=1.8 or later and omit DATAMAP.

If you specify RELEASE=1.7, or allow the release parameter to default to 1.7, the RACF manager returns data using the 1.7 user work area format. In this case, DATAMAP defaults to DATAMAP=OLD if you omit it.

If you want to use 1.8 parameters, and the 1.7 user work area format, you must specify RELEASE=1.8 or later and DATAMAP=OLD.

To use the 1.8 parameters, you must specify RELEASE=1.8 or later. If you specify RELEASE=1.8 or later the ICHEINTY parameter list must be in modifiable storage.

The default is RELEASE=1.7.

RUN =YES|NO

Specifies whether to activate or deactivate the parameter list. If you specify RUN=NO, the RACF manager ignores the request designated by this ICHEINTY macro although it will process the CHAIN parameter. If you specify RUN=YES, RACF processes this request and also processes the CHAIN parameter. Thus you can use the RUN parameter to deactivate or activate one or more ICHEINTY parameter lists without having to rearrange the chaining.

ACEE= acee-address

Specifies an ACEE that RACF uses to perform field authorization checking. If you specify FLDACC=YES, but omit ACEE, the RACF manager will use the appropriate ACEE pointed to either by the TCB or the ASXB.

WKSP= subpool-number

Specifies the number of a storage subpool. If the area specified by the WKAREA parameter is too small to contain the field data retrieved from LOCATE, NEXT, or NEXTC operation, the RACF manager obtains an additional workarea from this subpool in the caller's key. The RACF manager returns the address of the workarea in the fullword at offset 60 (X'3C') in the ICHEINTY parameter list. If additional storage is not needed, the RACF manager sets the

fullword to zero. It is your responsibility to free any returned workarea; its subpool number is stored in the one byte field at offset 29 (X'1D') in the parameter list, its address in the fullword at offset 60 (X'3C') in the ICHEINTY parameter list and its size in the first fullword of the workarea itself.

Notes:

1. Even if you specify WKSP, you must still provide a workarea at least 30 bytes long using the WKAREA operand.
2. You can simplify your coding if you use WKSP because you won't have to process a return code of 44 (X'2C').
3. If the RACF manager is unable to obtain a large enough workarea, an "out-of-storage" abend occurs.
4. You should take some care in selecting a subpool, as MVS makes certain assumptions about subpool usage and characteristics. In particular, using subpool 0, or 250, or any subpool documented in *z/OS MVS Programming: Assembler Services Guide* as having a storage key of USER (for example, 227–231, and 241) may give unpredictable results.

CHAIN= parm-list address

Specifies a parameter list that another ICHEINTY macro created. This chained parameter list executes after the current one within the same manager invocation. If several ICHEINTY requests pertain to the same profile, you can use CHAIN to string the requests together. This chaining improves performance because the RACF manager retrieves the profile only once for the entire chain. Each ICHEINTY parameter list in the chain must contain the same values for the following parameters: ACEE, CLASS, ENTRY or ENTRYX, GENERIC, RBA, SMC, TYPE, and VOLUME.

Notes:

1. Because there are no connect profiles in the database, chained ICHEINTY requests do not work as anticipated. Therefore, if you chain two ICHEINTY requests with TYPE=CON, the second ICHEINTY is ignored.
2. You cannot specify NEWNAME for any request in the chain.
3. When you chain ICHEINTY macros together, they must obey the following rules:
 - The first ICHEINTY in the chain must be a LOCATE, NEXT/NEXTC, ALTER/ALTERI, ADD, or a DELETE with SEGMENT specified.
 - The remaining ICHEINTY macros in the chain must be:
 - LOCATE, if the first was LOCATE
 - NEXT/NEXTC, if the first was NEXT or NEXTC
 - ALTERI, if the first was ALTERI
 - ALTER, if the first was ALTER, DELETE, or ADD
 - DELETE, with SEGMENT, if the first was ALTER or DELETE
 - The RACF manager return code will be set to the highest return code of any of the individual ICHEINTY macros that have been chained together.
 - For chained ICHEINTY parameter lists, within the bounds of any one chain of ICHEINTYs, an alias field (indicated by the alias bit in the fields template definition) may be referenced, either directly or indirectly (e.g. delete of a segment containing a defined alias field, or delete of a profile with a segment containing a defined alias field) multiple times. If there are multiple references, then there may be tests on any of these references

ICHEINTY Macro

except for the last reference. If a parameter list chain does not meet this requirement, return code 36 (X'24') reason code 11 (X'B') will be returned.

If an FLDEF test is specified for a delete or alter ICHEINTY whose last action on a specific alias field lacks a test, then unless there is an ICHEINTY parameter list earlier in the chain which also references the same alias field, then the FLDEF test does not count as a test on the last alias reference. This is because if the FLDEF test on the ICHEINTY fails, then none of the actions in the ICHEINTY parameter list will be executed.

DATAMAP= OLDINew (default depends on RELEASE)

DATAMAP determines the format of the workarea returned for a LOCATE, NEXT, or NEXTC operation and the format of the data you provide when you issue an ICHEINTY request to update the database. You can specify the DATAMAP parameter in several different combinations to tailor it to your system:

- If you specify RELEASE=1.7 or allow RELEASE= to default to 1.7, you need not specify DATAMAP. It defaults to OLD, meaning the 1.7 format.

Note: You cannot specify DATAMAP=NEW, if you specify RELEASE=1.7 or default to it.

- If you specify RELEASE=1.8 or later, and allow DATAMAP to default, it defaults to NEW, meaning the 1.8 format.
- If you specify RELEASE=1.8 or later, and want to use the 1.7 user work area format, you must specify DATAMAP=OLD for the data to be retrieved in the 1.7 format.

Note: Releases prior to 1.7 are in the 1.7 format.

SEGMENT= 'segment name'

Specifies that this request is to apply to a specific segment in the profile. If you do not specify a specific segment, the default is the BASE segment. If you specify a segment other than the BASE segment, the operation cannot be ADD, DELETEA, or RENAME. If you specify a segment, then the DELETE operation will delete only that segment. If you do not specify a segment, then the DELETE operation will delete the entire profile. If you specify a segment, then the ALTER operation will alter only that segment. If you do not specify a segment then the ALTER operation will update the BASE segment. See Appendix D, "RACF database templates" on page 391 for a list of valid segment names.

VOLUME= volume-address

Specifies the address of a 6-character volume identifier. When TYPE='DS', the volume identifier differentiates among data sets with the same name. When the operation is ADD, TYPE='GEN', and the class is TAPEVOL, the volume identifier specifies the name of an existing tape volume set to which the current entry is to be added. In all other cases, ICHEINTY ignores the volume identifier.

ACTIONS= (action-address,.....)

Specifies the address of one or more ICHEACTN macros that determine which profile field(s) the RACF manager is to retrieve or update. See the description of the ICHEACTN macro later in this chapter. You can specify up to 255 actions.

Note: If you specify ACTION on the execute form of the ICHEINTY macro, the number of actions you specify should agree with the number of actions you have specified on the list form of the macro (or the FLDEF list, if you

use that instead). If the numbers do not match, you must specify the OPTION keyword on the execute form to update the counts, using the appropriate ACTION operands.

TESTS= (test-addr,[AND],test-addr...)

Allows some preliminary testing on selected conditions prior to the execution of the operation specified by the ICHEINTY macro. You must specify an odd number of items (including the connector 'AND'). Each address must be the address of a list built by the ICHETEST macro. See "ICHETEST Macro" on page 329.

Note: If you specify TEST on the execute form of the ICHEINTY macro, the number of tests you specify should agree with the number of tests you have specified on the list form of the macro (or the FLDEF list, if you use that instead). If the numbers do not match, you must specify the OPTION keyword on the execute form to update the counts, using the appropriate TESTC or TESTM operands.

WKAREA= wkarea-address

Specifies the address of the area into which the retrieved values are to be placed. This operand is valid and required only for the LOCATE, NEXT, and NEXTC operations. The workarea must be at least 30 bytes long.

User work area formats are described under "Using ICHEACTN to Retrieve Data When ICHEINTY Has DATAMAP=NEW" on page 336 and "Using ICHEACTN to Retrieve Data When the ICHEINTY Has DATAMAP=OLD" on page 340. For a related operand, see the description of WKSP.

NEWNAME= newname-address

Specifies the address of the new name to be assigned to the entity named by the ENTRY operand. The name must be left-justified and followed by at least one blank.

Whereas ENTRY is a 1-byte length field followed by a name, NEWNAME specifies an entry name which is *not* preceded by a 1-byte length field. This operand is valid only for the RENAME operation.

When renaming resources in the FILE and DIRECTORY class, use ENTRYX and NEWNAMX. If NEWNAME is used, the name must be 39 characters long or less.

NEWNAMX= extended-newname-address

Specifies the address of the new name to be assigned to the entity in the ENTRYX keyword. The format of the new name is the same as that of the ENTRYX keyword.

- The first 2-byte field specifies a buffer length which can be from 0 to 255 bytes. This length field refers only to the length of the buffer that contains the entity name; it does not include the length of either length field.
- The second 2-byte field specifies the actual length of the entity name. This length field includes only the length of the actual name without any trailing blanks; it does not include the length of either length field.

NEWNAMX and NEWNAME are mutually exclusive parameters, as are NEWNAMX and WKAREA. The NEWNAMX keyword is valid only for the RENAME operation. To use NEWNAMX, you must specify RELEASE=1.9 or later.

RBA= RBA-address

Specifies the address of a 6-byte relative byte area (RBA) of a level one index

ICHEINTY Macro

that points to the profile to be altered. This keyword is valid only for an ALTERI request. RBA should specify the value returned by a previous LOCATE operation.

FLDEF= fldef-address

Specifies a remote list of ACTION/TEST pointers set up by an ICHEINTY with the FLDEF operation.

OPTIONS= ([NOPRO,TESTM,TESTC,ACTION,NOEXEC,FLDEF]...)

Provides more direct control of the code generated by the EXECUTE form of the macro. (This operand is valid only with the EXECUTE form of the macro.)

You can specify one or any number of the following subfields:

- | | |
|---------------|---|
| NOPRO | Does not generate any prologue code; that is, the instructions that set the type of request, such as ADD, by updating the first two bytes of the parameter list, are not generated. |
| FLDEF | Generates the FLDEF pointer relocation code to point to the list of ACTION and TEST pointers in the ICHEINTY macro expansion. |
| ACTION | Generates code to set the number of ACTIONs that are to be performed. |
| TESTC | Generates code to set the number of TESTs that are to be performed. |
| TESTM | Generates code to set both actual and maximum number of TESTs. |
| NOEXEC | Does not generate the SVC instruction to invoke the RACF manager. This subfield is useful with the EXECUTE form of the macro to allow partial setup of the parameter list. |

SMC= YESINO

Controls the 'set-must-complete' operation mode of the RACF manager. YES is the default mode of operation.

Note: If an ICHEINTY request is propagated by automatic direction of application updates, the SMC=NO keyword is not propagated. The ICHEINTY request will always run as SMC=YES on the target node.

GENERIC= NOIYESIUNCOND

Informs the RACF manager whether the given entity name is a generic name.

- | | |
|---------------|--|
| NO | Never generic.

The RACF manager does not attempt to convert the name specified by the ENTRY operand from external to internal form. GENERIC=NO is the default. |
| YES | May be generic.

The RACF manager attempts to convert the name specified by the ENTRY operand from external to internal form. The RACF manager does the conversion only if the entity name contains a generic character (an * or %). If the entity name does not contain a generic character, processing continues without any conversion. |
| UNCOND | Always generic.

The RACF manager unconditionally converts the name specified by the ENTRY operand from external to internal form. |

For RENAME, the same process applies also to the NEWNAME operand.

DATEFMT= YYYYDDDFIYYDDDF

Specifies the format of the date that you want to extract or replace.

If you specify DATEFMT=YYYYDDDF with a LOCATE, NEXT, or NEXTC operation, RACF retrieves date fields in the format *ccyydddF*, where *cc*=19 or *cc*=20. If an ADD, ALTER, or ALTERI operation is specified, RACF accepts dates in the format *ccyydddF*, where *cc*=19 or *cc*=20, unless the data being retrieved is in an un-initialized state in the RACF data base, in which case 0000000F or FFFFFFFF will be returned. When accepting a date as input to place into the database, RACF validates that *cc* is 19 or 20 and that:

- For *cc*=19, 70 < *yy* < = 99
- For *cc*=20, 00 < = *yy* < = 70

If you specify DATEFMT=YYDDDF, RACF retrieves and accepts dates in the three-byte format.

To specify the DATEFMT keyword, you must specify Release=1.9.2 or a later release number.

DATEFMT=YYDDDF is the default.

MF= ILLI(E,address)

Specifies the form of the macro as either INLINE, LIST, or EXECUTE.

The INLINE form generates code to branch around the parameter list. In the MF=I form, the label names the instruction preceding the parameter list. MF=I is the default.

The LIST form reserves and initializes storage.

The EXECUTE form modifies a list defined elsewhere. If you use the EXECUTE form, you must specify the address of the list to be modified. The address can be an A-type address or register (2 through 12).

Table 228. ICHEINTY Parameters

Parameter	RELEASE=1.7 and earlier	RELEASE=1.8 or later
ACEE		X
ACTIONS=	X	X
CHAIN=		X
CLASS=	X	X
DATAMAP=		X
ENTRY=	X	X
FLDACC		X
FLDEF=	X	X
GENERIC=	X	X
MF=	X	X
NEWNAME=	X	X
OPTIONS=	X	X
RBA=	X	X
RELEASE=	X	X

ICHEINTY Macro

Table 228. ICHEINTY Parameters (continued)

Parameter	RELEASE=1.7 and earlier	RELEASE=1.8 or later
RUN		X
SEGMENT		X
SMC=	X	X
TESTS=	X	X
TYPE=	X	X
VOLUME=	X	X
WKAREA=	X	X
WKSP		X

Return Codes from the ICHEINTY Macro

If you did not specify RELEASE=1.8 or later, Register 15 contains the ICHEINTY return code and Register 0 contains the reason code. If you specified RELEASE=1.8 or later, Register 15 contains the highest return code from any of the ICHEINTY macros; Register 0 contains the corresponding reason code. The return code for each ICHEINTY macro appears in the fullword at offset 52(X'34') in each ICHEINTY parameter list; the corresponding reason code appears in the fullword at offset 56(X'38').

Hex (Decimal) Description

0 (0)	The requested operation was successful.
4 (4)	If the reason code is 0, a recovery environment could not be established; if the reason code is 4, an invalid function code was specified. (Valid functions are RACLIST, RACXTRT, and ICHEINTY. The parameter list was not valid for any of those functions.)
8 (8)	An attempt was made to add an entry to the RACF database but an identical entry already exists.
C (12)	For requests other than NEXT or NEXTC, the specified entry did not exist. For NEXT or NEXTC requests, no subsequent entries satisfied the request.
10 (16)	Reserved.
14 (20)	The RACF database did not contain enough space to satisfy the request.
18 (24)	An I/O error occurred while accessing the RACF database.
1C (28)	RACF was not active at the time of the request.
20 (32)	The request type requires a user work area but the area was not provided (the address in the parameter list was 0) or for a RENAME, neither NEWNAME nor NEWNAMX was supplied.
24 (36)	The input parameter list or the associated ACTION and TEST blocks contain an error. When this code is returned, the possible reason codes are:

Code	Explanation
Hex (Decimal)	

ICHEINTY Macro

- 1 (1)** The entry name or new name is not valid
- 2 (2)** Action specified with DELETE or DELETEA
- 3 (3)** An action or test specified for an undefined field
- 4 (4)** Test specified with RENAME
- 5 (5)** Reserved
- 6 (6)** Reserved
- 7 (7)** Incorrect entry type
- 8 (8)** GROUP=YES specified for an ICHEACTN, but the data length given was too long for the associated data. This reason code can occur with DATAMAP=OLD.
- 9 (9)** GROUP=YES specified for an ICHEACTN, but the data length given was too short for the associated data.
- A (10)** Chained ICHEINTY macros have inconsistent parameters: (CLASS, ENTRY, ENTRYX, GENERIC, RBA, SMC, TYPE, or VOLUME).
- B (11)** Chained ICHEINTY macros have inconsistent request types (operations).
- C (12)** All ICHEINTY macros specified RUN=NO
- D (13)** Operation not allowed with SEGMENT keyword.
- E (14)** Illegal field specified for GROUP=YES, must be a repeat group count field
- F (15)** More than 1000 ICHEINTY macros present in the chain
- 10 (16)** Specified SEGMENT name not allowed for the specified profile type.
- 11 (17)** GROUP=YES specified for an ICHEACTN but the data length given was too long for the associated data. This reason code can occur with DATAMAP=NEW.
- 12 (18)** Data byte specified on ICHEACTN exceeded the length of the specified fixed-length field.
- 13 (19)** Inconsistency between action data length and repeat group fields. GROUP=YES data is too short.
- 14 (20)** Invalid ENTRYX. Current length is greater than 44 and either the primary or the backup database is not in the restructured database format.
- 15 (21)** Invalid NEWNAMX. Current length is greater than 44 and either the primary or the backup database is not in the restructured database format.
- 16 (22)** Data length specified on the ICHEACTN macro was less than zero and neither FLDATA=DEL nor FLDATA=COUNT were specified.

ICHEINTY Macro

- 17 (23)** Reserved.
- 18 (24)** Reserved.
- 19 (25)** Number of tests is greater than 254.
- 1A (26)** Invalid date supplied on an ICHEACTN when DATEFMT=YYYYDDDF is specified. Date must have a length of 4 bytes and in the form CCYYDDDF where CC=19, 70 < YY <= 99 and CC=20, 00 <= YY <= 70.
- 1B (27)** Repeat count cannot be updated when GROUP=NO is specified.
- 1C (28)** Alias locate requested but database is stage 0 or 1.
- 1D (29)** Invalid alias locate IPL.
- 1E (30)** Alias locate requested for a non-alias field.
- 1F (31)** Base pointer for test is 0 on an alias locate request.
- 20 (32)** Alias name length is 0 or greater than 252.
- 28 (40)** The maximum profile size (65,535 bytes) has been reached; the profile cannot be expanded.
- 2C (44)** The user-supplied work area was not large enough to hold all the data returned. The work area is filled with data up to, but not including, the first field that did not fit. If WKSP was specified, the manager obtains a new workarea, retrieves the data, and sets the return code to 0.
- 30 (48)** The user-supplied work area was smaller than the minimum amount required (30 bytes).
- 34 (52)** A test condition specified in the TESTS keyword of the ICHEINTY macro was not met; further processing was suppressed.
- 38 (56)** You requested an operation on a DATASET type entry that has multiple RACF definitions, but you did not specify a VOLUME to single out a specific entry.
- 3C (60)** For DATASET type entries, you specified a VOLUME that did not exist in the volume list of any entry with the specified name. For TAPEVOL class entries, a request tried to add a new TAPEVOL to a nonexistent tape volume set.
- 40 (64)** You attempted to delete one of the entries supplied by IBM (such as SYS1 or IBMUSER) from the RACF database.
- 44 (68)** An ALTERI request attempted to change the size of the profile being updated.
- 48 (72)** A request to add an entry to the RACF database would have caused the RACF index to increase to a depth that RACF does not support. The maximum depth is 10 levels.
- 4C (76)** ICHEINTY encountered an invalid index block or read a non-index block when it expected an index block.
- 50 (80)** An attempt was made to update one of the following (by a request other than ALTERI):
- The RACF database that has been locked by a RACF utility

ICHEINTY Macro

- The RACF database from a system that is in read-only mode (in a RACF sysplex data sharing environment)
- 54 (84)** Reserved.
- 58 (88)** At least one (but not all) ICHEACTN macros for information retrieval failed to be executed because of a profile field access violation.
- 5C (92)** All ICHEACTN macros for information retrieval failed to be executed because of a profile field access violation.
- 60 (96)** An ICHEACTN macro attempted to alter a field and failed because of a profile field access violation. All ICHEACTN macros for the ICHEINTY were suppressed. For FLDACC entries, the field class may not be active and processed by SETROPTS RACLIST.
- 64 (100)** The RELEASE keyword on the E-form ICHEINTY specified a release of 1.8 or later and CHECK, but the L-form did not specify a release of 1.8 or later.
- 68 (104)** The requested profile on the database contains erroneous data. A reason code is returned as follows:
- 1** The profile is physically too short to contain the data implied by variable field lengths or repeat group count fields.
- 6C (108)** The RACF manager has been invoked recursively, and an exclusive reserve/enqueue is required. However a shared reserve/enqueue is already held.
- 70 (112)** The RACF manager received an unexpected return code from a reserve/enqueue. The reserve/enqueue return code is passed back in register 0.
- 74 (116)** The maximum length of extended entry of ICHEINTY parameter list is not enough to contain a found profile name.
- 78 (120)** Reserved (used internal to RACF).
- 7C (124)** Reserved (used internal to RACF).
- 80 (128)** This is a data sharing mode return code. A coupling facility function had a problem when dealing with the ICB.
- 84 (132)** A request to expand an alias index entry beyond its maximum size has been denied.

ICHETEST Macro

The ICHETEST macro tests for user-specified conditions on selected data in a RACF profile. You can use the ICHETEST macro with the ICHEINTY and/or ICHEACTN macros to ensure that a specific requirement is met before processing of the ICHEINTY and/or ICHEACTN macro occurs. Failure to meet the requirements specified on the ICHETEST macro causes further processing of the associated ICHEINTY or ICHEACTN macro to be suppressed.

The ICHETEST macro must be issued from a task running in non-cross-memory mode with no locks held. The issuing task must be authorized (APF-authorized, in system key 0-7, or running in supervisor state).

The format of the ICHETEST macro is:

ICHETEST Macro

```
[label] ICHETEST FIELD=field-name|address
,FLDATA=(length,address)
[,COND=EQ|NE|GT|LT|GE|LE|ONES|ZEROS|
MIXED]
[,ENCRYPT=TEMPLATE|YES|NO]
[,MF=L|(E,address)|I]
[,RELEASE=number|(,CHECK)|(number,CHECK)]
```

FIELD= field-name|address

Specifies the field-name in the RACF profile whose value is to be tested.

If you use the LIST form of the macro, specify the name of the field. The name must be from 1-to 8-characters long, not enclosed in quotes, and defined in the RACF template. In addition, the field cannot be a combination field name (such as ACL in the group profile). Note, however, that a combination field that specifies only one associated field is allowable. Such a combination field is called an alias field such as OWNER in the GROUP profile.

If you use the EXECUTE or INLINE form of the macro, specify the address of the field name to be tested. The address can be an A-type address or register (2 through 12). For EXECUTE and INLINE, you can also specify the field name as a constant (for example, 'OWNER').

FLDATA= (length,address)

Specifies the data to be tested against.

The length must be greater than zero and less than or equal to the length of field-name in the FIELD operand, or the test will fail. For fixed length fields, you can specify a length that is less than the actual length of the field in the profile. For flag fields, the length specified is ignored and a 1-byte length is assumed. For variable-length fields, if the length is not equal to the field length in the profile, the test fails unless COND=NE is specified. Also, for variable-length fields the field data must not contain a length byte.

COND= EQ|NE|GT|LT|GE|LE|ONES|ZEROS|MIXED

Specifies the relationship that must exist between the FLDATA and FIELD values to satisfy the test. For example, COND=GE specifies that the value of FLDATA must be equal to or greater than the value of FIELD.

EQ, NE, GT, LT, GE, and LE are valid only for fixed length or variable-length fields. They are not valid for flag fields.

ONES, ZEROS, and MIXED are valid only for flag fields.

If you omit this operand, COND=EQ is the default. An explanation of ONES, ZEROS, and MIXED follows:

ONES If the 1 bits exist in the FIELD value base where the 1 bits exist in the FLDATA value, the test is successful.

ZEROS If the 0 bits exist in the FIELD value where the 1 bits exist in the FLDATA value, the test is successful.

MIXED If both 0 bits and 1 bits exist in the FIELD value where 1 bits exist in the FLDATA value, the test is successful.

You can think of this operation as being equivalent to doing a Test-Under-Mask operation. The ICHETEST data would be used as the mask, and the profile field would be used as the data.

ENCRYPT= TEMPLATE|YES|NO

Specifies whether the data specified by FLDATA is to be encoded before the test is performed. If ENCRYPT=YES, the data is encoded regardless of whether the template flag associated with the field specifies that it is to be encoded. If

ENCRYPT=NO, RACF does not encode the data regardless of the template flag value. If ENCRYPT=TEMPLATE, the template flag determines whether the data is encoded.

ENCRYPT is ignored if you specify COND as ONES, ZEROS, or MIXED.

MF= LI(E,address)l

Specifies the form of the macro as either LIST, EXECUTE, or INLINE.

The LIST form reserves and initializes storage. MF=L is the default.

The EXECUTE form modifies a list defined elsewhere. If you use the EXECUTE form, you must specify the address of the list to be modified. The address can be an A-type address or register (2 through 12).

The INLINE form is similar to a STANDARD form, except that it generates code to branch around the parameter list. In the MF=I form, the label names the first location of the parameter list, not the preceding instruction.

RELEASE=number

RELEASE=(,CHECK)

RELEASE=(number,CHECK)

Specifies the release number. The release numbers you can specify with the ICHETEST macro are 7707, 7706, 7705, 7703, 2608, 2.6, 2.4, 2.3, 2.2, 2.1, 1.9.2, 1.9, 1.8.1, 1.8, or 1.7.

Table 229. ICHETEST Parameters

Parameter	RELEASE=1.7 and earlier	RELEASE=1.8 or later
COND=	X	X
ENCRYPT=	X	X
FIELD	X	X
FLDATA	X	X
MF	X	X

Some considerations regarding the ICHETEST macros are:

- You cannot use the ICHETEST macro with an ICHEINTY macro that has the RENAME operation specified.
- A profile can contain repeat groups. A repeat group consists of one or more sequential fields that can be repeated in the profile. By specifying COND=EQ, you can select the occurrence of the repeat group to which the action applies. By specifying COND=NE, you can position yourself past the last occurrence of the repeat group. Then you can add a new occurrence to the end of that repeat group with an ICHEACTN macro.

Note: When the ICHEACTN macro refers to a repeat group and more than one ICHETEST macro is specified, the last ICHETEST macro serves to position data retrieval from the profile. Therefore, the last ICHETEST should refer to the same repeat group as the last ICHEACTN; otherwise the retrieved data will be from the last tested field. On multiple tests with fields in repeat groups, each test is processed separately, and if all succeed, the tests are considered to have succeeded.

- Tests involving negative numbers cause unpredictable results.
- If a specified address equals zero, ICHETEST makes no test.
- Use only COND=EQ or COND=NE to test masked fields. Other comparisons cause unpredictable results.

ICHETEST Macro

- The expansion of the ICHETEST macro MF=L or MF=I includes at offset 1, a 1-byte field whose value will be X'00' if the test was successful, or X'01' if the test failed. The ICHETEST parameter list must be in modifiable storage.
- If RELEASE=1.8 or later, the expansion of the ICHETEST macro MF=L or MF=I includes a one byte field at offset 3 whose low-order bit will be set to X'01' if the test failed because FLDACC=YES was specified on the associated ICHEINTY.
- It is possible to mix 1.7 and 1.8 or later format tests in the same request. The ICHEINTY and ICHEACTN macros can specify either RELEASE=1.7 or RELEASE=1.8 or later.
- When ICHEINTY LOCATE is used to retrieve data from a profile segment other than the BASE segment, default values (binary zeros for fixed-length fields, lengths of zero for variable length fields) will be returned by the manager if the profile could contain but does not contain an occurrence of that segment. If you need to know whether the segment actually exists, specify a TEST for the SEGNAME on the ICHEINTY. For example, when doing a LOCATE to retrieve the TSO segment from a user profile, use TEST as follows:

```
    ICHETEST  FIELD=SEGNAME,COND=EQ,FLDATA=(8,CTSO)
    .....
    .....
    CTSO  DC  CL8'TSO'
```

ICHEACTN Macro

You can use the ICHEACTN macro together with the ICHEINTY to retrieve or alter data in a specified RACF profile. ICHEACTN builds a parameter list containing the RACF profile field name and, optionally, the addresses of ICHETEST macros that control the data processing.

The ICHEACTN macro must be issued from a task running in non-cross-memory mode with no locks held. The issuing task must be authorized (APF-authorized, in system key 0-7, or running in supervisor state).

The format of the ICHEACTN macro is:

```
[label] ICHEACTN  FIELD=field-name|address
                  ,FLDATA=(length,address) | 'DEL' | 'COUNT'
                  [,TESTS=(address[,AND,address]...)]
                  [,RUN=YES|NO]
                  [,GROUP=YES|NO]
                  [,ENCRYPT=TEMPLATE|YES|NO]
                  [,MF=L|(E,address)|I]
                  [,RELEASE=number|(,CHECK)|(number,CHECK)]
```

FIELD=field-name|address

Specifies the field-name in the RACF profile whose value is to be retrieved or updated. The field must be one that is defined in the RACF database template.

Do not specify FIELD to be the first field in a database segment because the user cannot retrieve or update the first field in a segment. In the database templates, this field has a field ID of 001, and is usually described in the '**Field Being Described**' column as 'Start of Segment Fields'.

If you use the LIST form of the macro, specify the name of the field. The name must be 1-to 8-characters long, and not enclosed in quotes.

If you use the EXECUTE or INLINE form of the macro, specify the address of the name of the field to be retrieved or updated. The address can be an A-type address or register (2 through 12). For EXECUTE and INLINE, you can also specify the field name as a constant (for example, 'OWNER').

Do not alter a repeat group count field. Doing so causes unpredictable Results and could corrupt the profile.

FLDATA= (length,address)l'DEL'l'COUNT'

Updates or deletes data in a specified RACF profile. This operand is valid when used with the ALTER, ALTERI, ADD and RENAME operations on the ICHEINTY macro. It is also valid with LOCATE, NEXT or NEXTC if RELEASE=1.8 or later. The ICHEACTN macro will have eight bytes reserved to hold the length and address of the retrieved data. In no case will a LOCATE, NEXT, or NEXTC return data into a field whose address is given in the ICHEACTN macro.

When you use ICHEACTN to replace modify data, the address points to a field which contains the value that is to replace the data in the specified FIELD of the profile. The address may be an A-type address or general register ((2) through (12)). The length specifies the size of the replacement field, and must be an integer constant or register ((2) through (12)).

When you use ICHEACTN to retrieve data and you specify RELEASE=1.8 or later, the RACF manager places the size of the retrieved field in the word at offset 12(X'0C') and the address of the data in the word at offset 16(X'10') of the ICHEACTN parameter list if no tests are specified. The addresses specified in TESTS= are placed before the FLDATA entries within the parameter list. Therefore, for each address noted within TESTS=, the FLDATA entries are displaced by four bytes. The use of the TESTS= operand increments these offsets by four bytes for each test specified regardless of whether DATAMAP=NEW or DATAMAP=OLD is specified.

'DEL' causes the field named in the FIELD operand to be given a null value or causes an occurrence of a repeat group to be deleted, or (if GROUP=YES is coded) deletes all occurrences of a repeat group.

'COUNT' causes field-name in the FIELD operand to be treated as a positive integer and increased by one, unless the high-order bit is on, in which case, "COUNT" is reset to the value zero.

'COUNT' is intended for integer values only. Nor should 'COUNT' be used for repeat group count fields.

When replacing or adding data, the length and address are processed as follows:

- If DATAMAP=OLD is specified or defaulted on the ICHEINTY:
 - If the address is 0 or omitted, the specified field will be given a null value (a variable-length field is set to a length of 0; a flag field is set to X'00'; other fixed-length fields are set to all 'FF').
 - If the length is 0 or omitted, and the address is specified, the result depends upon whether the specified field is a variable-length field or a fixed-length field.
 - For a variable-length field, the field is given a null value. The length of the field is set to 0.
 - For a fixed-length field or a flag field, the field is given the value pointed to by the specified address. The length of the field is taken from the template.
- If DATAMAP=NEW is specified on the ICHEINTY:
 - If the length is 0 or omitted, or the address is 0 or omitted, the field is given a null value as indicated above. Otherwise, the field is set from the data specified, with the length specified. For a fixed-length field, if the specified length is less than the length given in the template, the value will be left-adjusted and filled with X'00's to the template length. If the length is

ICHEACTN Macro

greater than the template length, the operation will fail. For variable-length fields, the specified length is used; the first byte of the data is not used as the data length, but rather is considered to be data.

TESTS= (address[, [AND], address]...)

Specifies preliminary testing that must occur before any data retrieval or updating takes place. Each address specified must be the address of a list built by an ICHETEST macro. The address can be an A-type address or register (2 through 12). Multiple addresses indicate that all conditions (tests) must be satisfied. If not, RACF suppresses further processing of the macro. If you omit the logical connector 'AND', you must use a comma to indicate its omission.

Note: If GROUP=YES is also coded on the ICHEACTN macro, all tests specified by the TESTS parameter are ignored unless RELEASE=1.8 or later is also specified.

The addresses specified in TESTS= are placed before the FLDATA entries within the parameter list. Therefore, for each address noted within TESTS=, the FLDATA entries are displaced by four bytes. The use of the TESTS= operand increments these offsets by four bytes for each test specified regardless of whether DATAMAP=NEW or DATAMAP=OLD is specified.

RUN= YESINO

Specifies if a data retrieval or update is to be actually performed. This operand allows you to code an ACTION operand on the ICHEINTY macro without the action being performed for this particular execution. The default is RUN=YES.

GROUP= YESINO

Specifies whether an update for a repeat group is for a single occurrence of the group or for the entire group, including the repeat count that contains the number of occurrences. If FIELD=field-name contains the name of a repeat group count field and GROUP=YES, ICHEACTN replaces or deletes the entire repeat group, including the count field. The data format used with GROUP=YES depends on the DATAMAP value on the ICHEINTY. See "Using ICHEACTN to Alter Data When the ICHEINTY Has DATAMAP=NEW" on page 339 and "Using ICHEACTN to Alter Data When ICHEINTY Has DATAMAP=OLD" on page 342 for details.

Note: If GROUP=YES is also coded on the ICHEACTN macro all tests specified by the TESTS parameter are ignored unless RELEASE=1.8 or later is specified.

ENCRYPT= TEMPLATEIYESINO

Specifies whether the data specified by FLDATA is to be encoded. If ENCRYPT=YES, the data is encoded regardless of whether the template flag associated with the field specifies that it is to be encoded. If ENCRYPT=NO, RACF does not encode the data regardless of the template flag value. If ENCRYPT=TEMPLATE, the template flag determines whether the data is encoded.

MF= LI(E,address)II

Specifies the form of the macro as either LIST, EXECUTE or INLINE.

The LIST form reserves and initializes storage. MF=L is the default. If RELEASE=1.8 or later is specified, the storage must be modifiable, that is, not within a re-entrant module.

The EXECUTE form modifies a list defined elsewhere. If you use the EXECUTE form, you must specify the address of the list to be modified. The address can be an A-type address or register (2 through 12).

The INLINE form is similar to a STANDARD form, except that it generates code to branch around the parameter list. In the MF=I form, the label names the first location of the parameter list, not the preceding instruction.

RELEASE=number

RELEASE=(,CHECK)

RELEASE=(number,CHECK)

Specifies the release number.

The release numbers you can specify with the ICHEACTN macro are 7707, 7706, 7705, 7703, 2608, 2.6, 2.4, 2.3, 2.2, 2.1, 1.9.2, 1.9, 1.8.1, 1.8, or 1.7.

When you specify 1.8 or later, the RACF manager returns data using the new 1.8 user work area format (documented under the section entitled “Using ICHEACTN to Retrieve Data” in this chapter). In effect, DATAMAP defaults to DATAMAP=NEW, if you specify RELEASE=1.8 or later and omit DATAMAP.

If you specify RELEASE=1.7 or allow the release parameter to default to 1.7, the RACF manager returns data using the 1.7 user work area format. In this case, DATAMAP defaults to DATAMAP=OLD if you omit it.

If you want to use 1.8 parameters, and the 1.7 user work area format, you must specify RELEASE=1.8 or later and DATAMAP=OLD.

To use the 1.8 parameters, you must specify RELEASE=1.8 or later. If you specify RELEASE=1.8 or later, the ICHEINTY parameter list must be in modifiable storage. The parameter list will include at offset 3 a byte whose low order bit (X'01') will be set if the action failed because of field level access checking.

The default is RELEASE=1.7.

Table 230. ICHEACTN Parameters

Parameter	RELEASE=1.7 and earlier	RELEASE=1.8 or 1.8.1
ENCRYPT=	X	X
FIELD=	X	X
FLDATA=	X	X
GROUP=	X	X
MF=	X	X
RUN=	X	X
TESTS=	X	X

Using ICHEACTN With the DATAMAP=NEW and DATAMAP=OLD Operands

With Release 1.8, installations can choose between using their old datamap format and the new 1.8 datamap format. The following sections explain the relationship between the DATAMAP keyword and the RELEASE keyword. In addition, this section explains how to use the ICHEACTN to retrieve and alter data when the ICHEINTY macro has DATAMAP=NEW specified and how to use ICHEACTN when the ICHEINTY macro has DATAMAP=OLD specified.

ICHEACTN Macro

Using ICHEACTN to Retrieve Data When ICHEINTY Has DATAMAP=NEW

The ICHEACTN macro retrieves data when used with the ICHEINTY macro which has a LOCATE, NEXT or NEXTC operand. With DATAMAP=NEW on the ICHEINTY and RELEASE=1.8 or later on the ICHEACTN, data retrieval and modification are compatible operations. That is, you can do an ICHEINTY LOCATE followed by an ICHEINTY ALTER (with the same ICHEACTN) and the profile will end up with its original data. Or alternatively, by changing the ENTRY name you could copy data from one profile to another. When using ICHEACTN to retrieve data, you must supply a work area on the ICHEINTY macro into which the retrieved data can be placed. The first fullword of the work area must be the length of the work area (including the first fullword itself). The minimum work area is 30 bytes, even if no data is being retrieved.

The format of the user work area is as follows:

Offset (hex)	Length	Description
0	4	Length of entire work area
4	6	RBA return area
A	1	Flags
B	1	Reserved
C	4	Duplicate data set name count
10	8	Reserved
18	4	Length of data returned into work area
1C	variable	Field value return area

Ensure that the storage in the work area from +4 to +1E is initialized to binary zeros. If the area is not initialized, it can be difficult to determine if the information returned by the RACF manager is present.

If the profile located has a generic name, bit 0 (X'80') of the flag byte at offset (X'0A') is set to on.

An ICHEINTY macro can have several ICHEACTN macros associated with it. For each ICHEACTN macro, the RACF manager returns into the field value return area:

- A 4-byte length field. This length field contains the length of the retrieved data for that particular ICHEACTN macro. Note that this 4-byte length field does not contain its own length.
- The retrieved data from the RACF profile.
 - Simple variable-length fields are not preceded by an additional length byte as in the old format.
 - Within a combination field, each field is preceded by its respective four byte length field.
 - An alias field (combination field made up of only one field) does not have an extra length field.
 - Repeat group count fields are four bytes long, not two.
 - When replacing or retrieving an entire repeat group using (GROUP=YES), the repeat group count field does not precede the data.

When multiple ICHEACTNs are used, each returns data immediately following the data (if any) returned by the preceding ICHEACTN.

Note that all the fields are byte-aligned. In addition, if the ICHEACTN contains RELEASE=1.8 or later, the manager places the data length in the fullword at offset

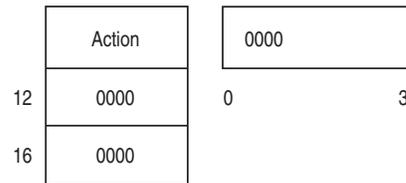
12(X'0C') of the ICHEACTN and places a pointer to the data in the fullword at offset 16(X'10') of the ICHEACTN parameter list if no tests are specified. You must increment these offsets by 4 for each test specified by the ICHEACTN TESTS= parameter.

For example, with two tests, the length is returned at X'14' and the address is returned at X'18'. The addresses specified in TESTS= are placed before the FLDATA entries within the parameter list. Therefore, for each address noted within TESTS=, the FLDATA entries are displaced by four bytes.

The use of the TESTS= operand increments these offsets by four bytes for each test specified regardless of whether DATAMAP=NEW or DATAMAP=OLD is specified. The following examples show the format of the returned data (and the values that would be placed in the ICHEACTN if you specify RELEASE=1.8 or later).

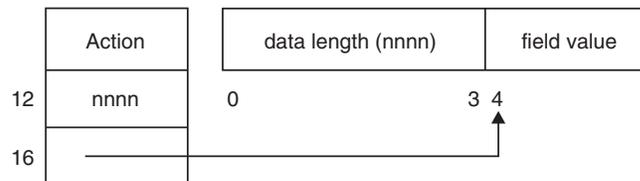
Some examples of the different field types that the RACF manager can return in the field value return area are:

1. If a condition specified by an ICHETEST macro (that is associated with the ICHEACTN macro) was not satisfied or if the specified field was a repeat field that contained no members, or if the action was failed by field level access checking, the field value area will not be returned and the length area will be equal to X'00000000'.



2. If the field specified is a fixed-length field, a variable-length field, a flag field, or a repeat group count field (GROUP=NO), the return field contains the length of the field followed by the field value.

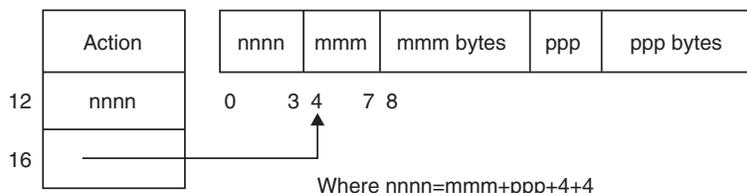
Note: A flag field is always one byte long. A repeat group count field is always four bytes long if GROUP=NO. An alias field is processed the same way as the simple field of which it is an alias.



3. If the field specified is a combination field, the return area contains the length of all the fields in the combination, followed by a concatenation of the individual simple fields in the combination. Each simple field is returned as described above in (2).

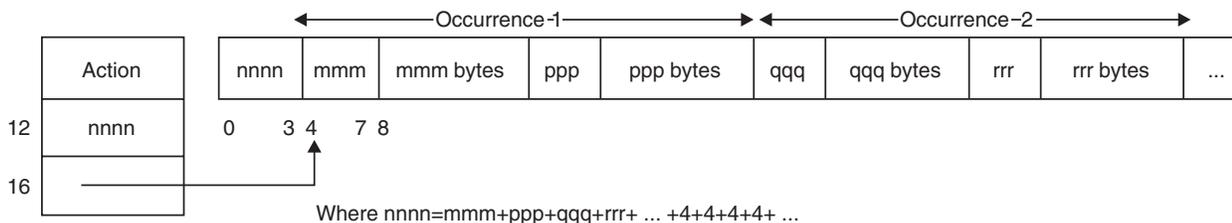
For example, if the combination contains two simple fields:

ICHEACTN Macro

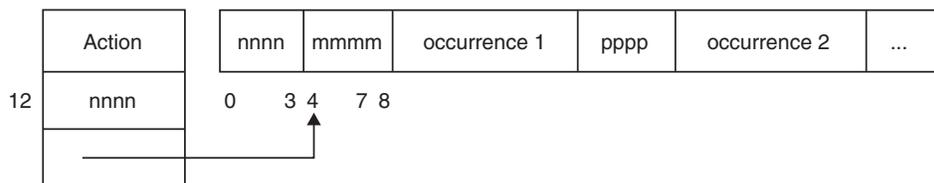


4. If the field specified is a field in a repeat group or a combination field made up of one or more fields in the same repeat group, the results returned depend upon whether
 - An ICHETEST macro was associated with the ICHEACTN in order to position to a particular occurrence of the repeat group or
 - No ICHETEST macro was associated and all occurrences are implied.

When an ICHETEST is associated, the format of the result is the same as if the field were not in a repeat group. When no ICHETEST is associated, the result is the four-byte length field followed by the concatenation of the values of every occurrence of the specified field in the format shown above. If the specified field is a combination field, the values of the fields in the combination are first concatenated for each occurrence, then these concatenations are concatenated in the order of their occurrence.



5. If the field is a repeat-group count field, and the ICHEACTN specifies GROUP=YES, then the retrieved data contains all occurrences of the repeat group, in the following format:



Where nnnn is the total length of data returned, mmmm is the length of occurrence 1, and pppp is the length of occurrence 2.

Each occurrence will be formatted as though it were a combination field (see example 3 on page 337) of all template fields defined for the group. For example, data set profiles have a field called ACLCNT; the fields in the group are USERID, USERACS, and ACSCNT. An ICHEACTN to retrieve ACLCNT, with GROUP=YES, would return the following data if ACLCNT has the value 2:

nnnn (length of data)	DC AL4(54)
mmmm (length of occurrence 1)	DC AL4(23)
Declares for occurrence 1	DC AL4(8)
	DC CL8 'userid1'
	DC AL4(1)

```

                DC AL1(useracs1)
                DC AL4(2)
                DC AL2(acscnt1)
pppp (length of occurrence 2)  DC AL4(23)
Declares for occurrence 2     DC AL4(8)
                               DC AL4(8)
                               DC CL8'userid2'
                               DC AL4(1)
                               DC AL2(useracs2)
                               DC AL4(2)
                               DC AL2(acscnt2)

```

Using ICHEACTN to Alter Data When the ICHEINTY Has DATAMAP=NEW

The ICHEACTN macro alters data when used with the ICHEINTY macro having an ADD, ALTER, ALTERI, or RENAME operand. If the conditions specified by the TESTS keyword on the ICHEACTN macro are met, the field specified in the FIELD operand is assigned the value specified in the FLDATA operand. If the specified field in the RACF profile is in a repeat group, then:

- If you specified a test with COND=EQ, the existing occurrence of the repeat group is altered.
- If you specified a test with COND=NE, a new occurrence is added to the end of the repeat group.
- If you did not specify a test, a new occurrence is added to the beginning of the repeat group.

When replacing data, the FLDATA parameter should describe the size of the data and its address in the same format as shown above for retrieving data. When specifying a combination field, the total size must equal the sum of the individual sizes, including the length fields or the request fails.

The specification of FLDATA='COUNT' causes the specified fields to be treated as a positive integer and increased by one. If the field specified is variable length or has a fixed length greater than four, RACF ignores the specification and does not modify the field value.

If you specify FLDATA='DEL', the specified field has a null value; that is:

- For a fixed-length field that is not in a repeat group, the field is set to binary ones.
- For a flag field that is not in a repeat group, the field is set to binary zeros.
- For variable-length fields that are not in a repeat group, the length of the field is set to zero.
- For fields within a repeat group, the entire occurrence is deleted.

If you specify zero as the "address" value, the result is the same as if you had specified FLDATA='DEL', except that for fields in a repeat group, the field in the occurrence is set to a null value (the same as fields not in a repeat group).

If you specify FLDATA='DEL' or FLDATA='COUNT' on an ICHEACTN, the length field of the ICHEACTN is set to -1 or -2. If you also specify RELEASE=1.8 or later, and subsequently use the ICHEACTN to retrieve data, these new values will be lost. To avoid this, you should not use the same ICHEACTN for both DEL/COUNT and retrieval processing; or you should use the E-Form to re-establish DEL/COUNT after the data retrieval.

ICHEACTN Macro

Using ICHEACTN to Retrieve Data When the ICHEINTY Has DATAMAP=OLD

The ICHEACTN macro retrieves data when used with the ICHEINTY macro having a LOCATE, NEXT or NEXTC operand. When using ICHEACTN to retrieve data, you must supply a work area on the ICHEINTY macro into which the retrieved data can be placed. The first fullword of the work area must be the length of the work area (including the first fullword itself). The minimum work area is 30 bytes, even if no data is being retrieved.

The format of the user work area is as follows:

Offset (hex)	Length	Description
0	4	Length of entire work area
4	6	RBA return area
A	1	Flags
B	1	Reserved
C	4	Duplicate data set name count
10	8	Reserved
18	4	Length of data returned into work area
1C	variable	Field value return area

Ensure that the storage in the work area from +4 to +1E is initialized to binary zeros. If the area is not initialized, it can be difficult to determine if the information returned by the RACF manager is present.

If the profile located has a generic name, bit 0 (X'80') of the flag byte at offset (X'0A') is on. This flag bit is useful when performing NEXT or NEXTC operations to process many profiles.

An ICHEINTY macro can have several ICHEACTN macros associated with it. For each ICHEACTN macro, the RACF manager returns into the field value return area:

- A 2-byte length field. This length field contains the length of the retrieved data for that particular ICHEACTN macro. Note that this 2-byte length field does not contain its own length.
- The retrieved data from the RACF profile.

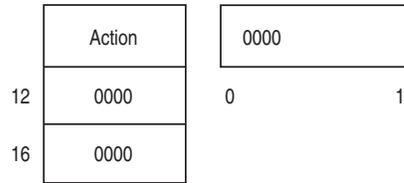
Note that all the fields are byte-aligned. In addition, if the ICHEACTN contains RELEASE=1.8 or later, the manager will place the data length in the fullword at offset 12(X'0C') of the ICHEACTN, and will place a pointer to the data in the fullword at offset 16(X'10') of the ICHEACTN parameter list if no tests are specified. You must increment these offsets by 4 for each test specified by the ICHEACTN TESTS= parameter.

For example, with two tests, the length is returned at X'14' and the address is returned at X'18'. The addresses specified in TESTS= are placed before the FLDATA entries within the parameter list. Therefore, for each address noted within TESTS=, the FLDATA entries are displaced by four bytes. The use of the TESTS= operand increments these offsets by four bytes for each test specified regardless of whether DATAMAP=NEW or DATAMAP=OLD is specified.

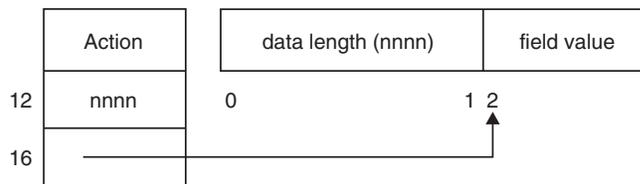
The following examples show the format of the returned data (and the values that would be placed in the ICHEACTN if you specify RELEASE=1.8 or later).

Some examples of the different field types that the RACF manager can return in the field value return area are:

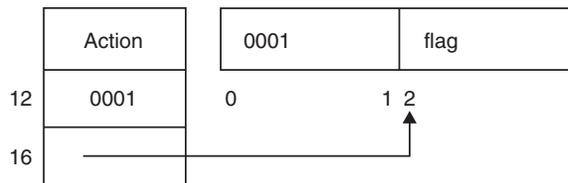
1. If a condition specified by an ICHETEST macro (that is associated with the ICHEACTN macro) was not satisfied or if the specified field was a repeat field that contained no members, the field value area will not be returned and the length area will be equal to X'0000'.



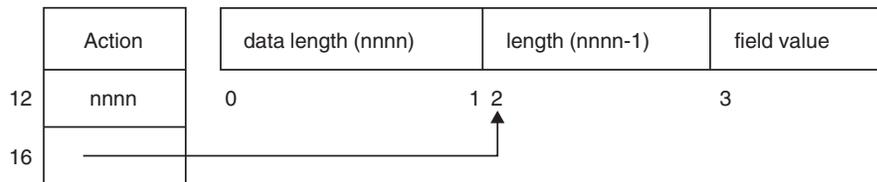
2. If the field specified is a fixed-length field, the return field contains the length of the field followed by the field value.



3. If the field specified is a flag field, the return field contains the length of the field (X'0001') followed by a 1-byte value.

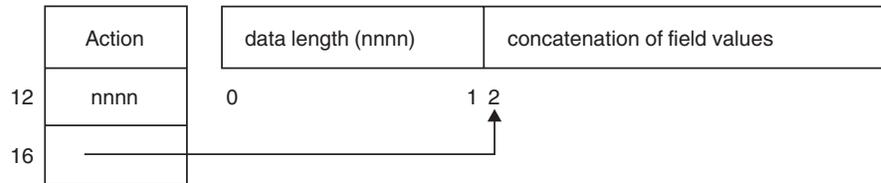


4. If the field specified is a variable-length field, the return field contains the length of the field followed by a 1-byte length field (that does not include its own length) followed by the field value.



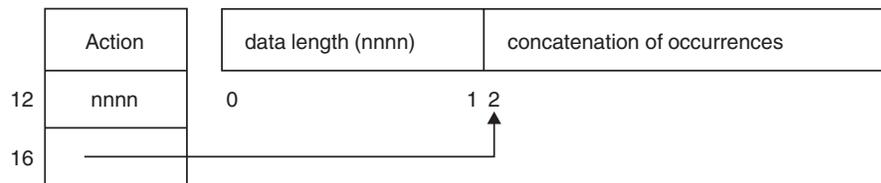
5. If the field specified is a combination field, the return area contains the length of all the fields in the combination, followed by a concatenation of values of each of the individual fields in the combination. If a field in the combination is in a repeat group, all the fields in the combination must be in the same repeat group. (Example 6 shows how the RACF manager returns combinations containing fields of a repeat group.)

ICHEACTN Macro



6. If the field specified is a field in a repeat group or a combination field made up of one or more fields in the same repeat group, the results returned depend on whether (1) an ICHETEST macro was associated with the ICHEACTN in order to position to a particular occurrence of the repeat group or (2) no ICHETEST macro was associated and all occurrences are implied.

When an ICHETEST is associated, the format of the result is the same as if the field were not in a repeat group. When no ICHETEST is associated, the result is the two-byte length field followed by the concatenation of the values of every occurrence of the specified field. If the specified field is a combination field, the values of the fields in the combination are first concatenated for each occurrence, then these concatenations are concatenated in the order of their occurrence.



Using ICHEACTN to Alter Data When ICHEINTY Has DATAMAP=OLD

The ICHEACTN macro alters data when used with the ICHEINTY macro having an ADD, ALTER, ALTERI, or RENAME operand. If the conditions specified by the TESTS keyword on the ICHEACTN macro are met, the field specified in the FIELD operand is assigned the value specified in the FLDATA operand. If the specified field in the RACF profile is in a repeat group, then:

- If you specified a test with COND=EQ, the existing occurrence of the repeat group is altered.
- If you specified a test with COND=NE, a new occurrence is added to the end of the repeat group.
- If you did not specify a test, a new occurrence is added to the beginning of the repeat group.

RACF uses the length specified as a subfield of the FLDATA keyword only when you specify GROUP=YES. For fixed-length fields, the data length is the field length in the template. For variable-length fields, the data length is the first data byte (it does not include its own length). RACF handles combination fields as a succession of fields, either fixed or variable length. If the combination field contains some but not all of the fields in a repeat group, the fields not included are set to null values.

The specification of FLDATA='COUNT' causes the specified field to be treated as a positive integer and increased by one. If the field specified is variable length or has a fixed length greater than four, RACF ignores the specification and does not modify the field value.

If you specify FLDATA='DEL', the specified field is given a null value; that is:

- For a fixed-length field that is not in a repeat group, the field is set to binary ones.
- For a flag field that is not in a repeat group, the field is set to binary zeros.
- For variable-length fields that are not in a repeat group, the length of the field is set to zero.
- For fields within a repeat group, the entire occurrence is deleted.

If you specify zero as the “address” value, the result is the same as if you had specified `FLDATA='DEL'`, except that for fields in a repeat group, the field in the occurrence is set to a null value (the same as fields not in a repeat group).

Examples of ICHEINTY, ICHECTEST, and ICHEACTN Macro Usage

The following examples illustrate some of the functions provided by the ICHEINTY, ICHECTEST, and ICHEACTN macros:

1. Determining if a user is defined to RACF

```

*      .
*      .
*      .
      LA   15,WEND-W      LENGTH OF WORK AREA.
      ST   15,W           INITIALIZE WORK AREA.
      XC   WR,WR          CLEAR RESERVED AREA.
      ICHEINTY LOCATE,TYPE='USR',ENTRY=USR1,WKAREA=W
      LTR  15,15          R15=0 IF USER DEFINED TO
                          RACF
      BNZ  NOTDEFD
*      .
*      .
*      .
*      DATA AREAS
USR1   DS   AL1          LENGTH OF USERID (1 TO 8)
        DS   CL8          USERID
W      DS   0F
        DS   F            LENGTH OF WORK AREA.
WR     DS   CL24         RESERVED.
        DS   F
WEND   EQU  *           END OF WORK AREA.

```

The ICHEINTY macro identifies the user profile to be located. A return code of 0 (X'00') in register 15 indicates that the user is defined to RACF. A return code of 12 (X'0C') indicates that the user is not defined. Note that this ICHEINTY macro contains a work area. By also coding an ICHEACTN macro in this example, you can retrieve current field values from this user profile into the work area.

2. Adding a user ID to a data set access list

```

*      .
*      .
*      .
      ICHEINTY ALTER,TYPE='DS',ENTRY=DSN1,          *
          ACTIONS=AACL
      LTR  15,15          0 RETURNED IF DS IS RACF
                          DEFINED
      BNZ  DSNOTDEF      DS NOT RACF DEFINED OR
                          ERROR
      CLI  TUSERID+1,X'00' WAS USER ALREADY IN LIST
      BNZ  INLIST        YES. USER WAS IN LIST
                          ALREADY
*      .
*      .

```

Examples

```

*      .
*      DATA AREA
AACL   ICHEACTN FIELD=ACL,FLDATA=(11,ACL),          *
        TESTS=TUSERID,MF=L
TUSERID ICHETEST FIELD=USERID,FLDATA=(8,USER),COND=NE, *
        MF=L
DSN1   DS     AL1          DATA SET NAME LENGTH
        (1 TO 44)
        DS     CL44        DATA SET NAME
ACL     DS     0CL11       ACCESS LIST ENTRY
USER    DS     CL8         USERID TO BE ADDED
USERACS DS     XL1         ACCESS TO BE GIVEN:
*                               X'80' FOR ALTER
*                               X'40' FOR CONTROL
*                               X'20' FOR UPDATE
*                               X'10' FOR READ
*                               X'01' FOR NONE
ACSCNT  DC     XL2'0000'   ZERO ACCESS COUNT

```

The ICHEINTY macro identifies the data set profile whose access list is to be updated. It also points to an ICHEACTN macro that describes how the profile is to be updated. In this example, RACF adds a user ID to the access list.

The ICHEACTN macro, in turn, points to an ICHETEST macro that tests for certain conditions before the profile can be updated. In this example, ICHETEST tests to determine if the specified user ID already exists in the access list. (The second byte of the test block at TUSERID is 0 if the user ID is not in the access list.) If the user ID does not exist, RACF adds the user ID (with the specified access authority) to the access list and updates the data set profile. If the user ID already exists, no profile update occurs.

3. Changing the access authority of a user in a data set access list

```

*      .
*      .
*      .
*      ICHEINTY ALTER,TYPE='DS',ENTRY=DSN1,          *
        ACTIONS=AUSRACS
LTR    15,15          0 RETURNED IF DS IS RACF
        DEFINED
BNZ    DSNOTDEF       DS NOT RACF DEFINED OR
        ERROR
CLI    TUSERID+1,X'00' WAS USER IN LIST
BNZ    NOTINLST       NO. USER WAS NOT IN
        LIST
*      .
*      .
*      .
*      DATA AREA
AUSRACS ICHEACTN FIELD=USERACS,FLDATA=(1,USERACS), *
        TESTS=TUSERID,MF=L
TUSERID ICHETEST FIELD=USERID,FLDATA=(8,USER),COND=EQ, *
        MF=L
DSN1   DS     AL1          DATA SET NAME LENGTH
        (1 TO 44)
        DS     CL44        DATA SET NAME
UACC   DS     XL1         ACCESS TO BE GIVEN:
*                               X'80' FOR ALTER
*                               X'40' FOR CONTROL
*                               X'20' FOR UPDATE
*                               X'10' FOR READ
*                               X'01' FOR NONE

```

This example is similar to the previous example. However, if the user ID exists in the data set access list, RACF changes that user's access authority to the value specified in USERACS and updates the data set profile. If the user ID does not exist, no profile update occurs.

Note that you can use this example to delete a user ID from the data set access list by changing the ICHEACTN macro to read:

```
AUSRACS ICHEACTN FIELD=USERID,FLDATA='DEL',          *
        TEST=TUSERID,MF=L
```

4. Retrieving owner names of all data set profiles

The following example program shows an ICHEINTY coded to retrieve the owner names of all data set profiles in the RACF database.

```
EXAMPLE CSECT
*
*      entry linkage
*
      STM 14,12,12(13)          push caller registers
      BALR 12,0                establish ...
      USING *,12                ... addressability
      GETMAIN R,LV=DYNLEN      get dynamic storage
      LR 11,1                   move getmained address to R11
      USING DYNAREA,11         addressability to DSECT
      ST 13,SAVEAREA+4        save caller save area address
      LA 15,SAVEAREA          get address of own save area
      ST 15,8(13)             store in caller save area
      LR 13,15                 get address of own save area
*
*      initialize variables in dynamic storage area
*
      MVC ENTBLEN,H44          set buffer length to 44
      MVC ENTNLEN,H1           set entity length to 1
      XC ENTNAME,ENTNAME       clear entity name area
      MVC RETALEN,F40          set return area length
*
*      copy static ICHEINTY and ICHEACTN to dynamic GETMAINED areas
*
      MVC DYNICH(ICHLEN),STATIC
      MVC DYNACT(ACTLEN),STACT
      ICHEINTY RELEASE=1.9,ACTIONS=(DYNACT),WKAREA=RETAREA,      *
        OPTIONS=(FLDEF,NOEXEC),GENERIC=NO,MF=(E,DYNICH)
*
*      loop to retrieve all data set profiles
*      for each high level qualifier, generic profiles are
*      retrieved first
*
LOOP EQU *                    start of loop
      XC RETDATA,RETDATA      clear ICHEINTY return data
      ICHEINTY NEXTC,ENTRYX=ENTBUFF,RELEASE=1.9,MF=(E,DYNICH)
      LTR 15,15               check return code
      BNZ DONE                exit on non zero return code
*
*      .
*
*      process data set profiles
*
*      .
*
      TM RETFLAGS,X'80'       check generic bit
      BO GENERIC              branch if generic bit is on
      ICHEINTY OPTIONS=(NOEXEC),GENERIC=NO,MF=(E,DYNICH)
      B LOOP                  process next profile
*
GENERIC EQU *                 profile name is generic
      ICHEINTY OPTIONS=(NOEXEC),GENERIC=UNCOND,MF=(E,DYNICH)
```

Examples

```

        B      LOOP                process next profile
*
*      return to caller
*
DONE    EQU    *                  return to caller
        L      13,SAVEAREA+4      caller's save area address
        FREEMAIN R,LV=DYNLEN,A=(11) free dynamic storage
        LM     14,12,12(13)       pop registers
        SLR    15,15              clear return code
        BR     14                  return to caller
*
*      static ICHEACTN and ICHEINTY areas
*
STATACT ICHEACTN FIELD=OWNER
ACTLEN  EQU    *-STATACT          length of ICHEACTN
*
STATICH ICHEINTY NEXTC,TYPE='DS',ENTRYX=-*,RELEASE=1.9,DATAMAP=NEW, *
        ACTIONS=(STATACT),WKAREA=-*,MF=L
ICHLEN  EQU    *-STATICH          length of ICHEINTY
*
*      constants
*
H1      DC     H'1'
H44     DC     H'44'
F40     DC     F'40'
*
*      dynamic area
*
DYNAREA DSECT
*
SAVEAREA DC    18F'0'
DYNICH   DS    17F                dynamic ICHEINTY area
DYNACT   DS    6F                dynamic ICHEACTN area
*
*      ENTITYX structure
*
ENTBUFF  DS    0CL48
ENTBLEN  DS    H
ENTNLEN  DS    H
ENTNAME  DS    CL44
*
*      return work area
*
RETAREA  DS    0CL40
RETALEN  DS    F                  return area length
RETDATA  DS    0CL36
RETRBA   DS    CL6               RBA return area
RETFLAGS DS    CL1              flags
RETRES1  DS    CL1              reserved
RETDDSC  DS    F                duplicate data set name count
RETRES2  DS    CL8              reserved
RETDLEN  DS    F                returned data length
RETOWNLN DS    F                returned owner name length
RETOWNER DS    CL8              returned owner name
*
DYNLEN   EQU    *-DYNAREA        dynamic area length
*
        END
```

5. Updating the “Installation Fields”

The RACF template defines a repeat group of fields for installation use. There are four of these fields:

- USRCNT** Contains the number of repeat members in the group. A repeat member is one USRNM field, one USRDATA field, and one USRFLAG field.
- USRNM** Describes the contents of the USRDATA field.
- USRDATA** Contains any information that you choose.
- USRFLAG** Is a flag associated with USRNM.

The following example shows how the installation fields are used:

```
USRCNT = 2
      USRNM  ACCTNMBR
      USRDATA K83-1234/DQ3
      USRFLG  00

      USRNM  ADDRESS
      USRDATA RFD 4, Box 7711, Phoenicia, NY
      USRFLG  00
```

The following example shows how to add or update a repeat group member. This code will first delete an existing occurrence, based on the name in USRNM, and then add a new occurrence with the desired new (or updated) data. The code is assumed to be preceded by code that initializes the UDATANM, UDATAL1 and UDATAV fields.

In the part of the example not shown, the ACTN3 and ACTN4 macros are addressed by an ICHEINTY-ALTER macro. The ACTN3 and ACTN4 macros must be specified in the ICHEINTY-ACTIONS keyword in the order ACTN3,ACTN4.

```
ICHEACTN MF=(E,ACTN3),TESTS=TEST3
ICHETEST MF=(E,TEST3),FLDATA=(,UDATANM)
ICHEACTN MF=(E,ACTN4),FLDATA=((Rx),UDATA),TESTS=TEST4
ICHETEST MF=(E,TEST4),FLDATA=(,UDATANM)
.
.
.
--- Invoke ICHEINTY ---
.
.
.
ACTN3  ICHEACTN FIELD=USRNM,FLDATA='DEL',TESTS=-*-
TEST3  ICHETEST FIELD=USRNM,FLDATA=(8,*-*)          COND=EQ is default.
ACTN4  ICHEACTN FIELD=USRDATA,FLDATA=(*-*,*-*),TESTS=-*-

TEST4  ICHETEST FIELD=USRNM,FLDATA=(8,*-*),COND=NE

UDATA  DS      0C           Start of USERDATA area.
UDATANM DS     CL8         Contents of USRNM field.
UDATAL1 DS     AL1         Length of USRDATA field.
UDATAV DS     CL--        Contents of USRDATA field.
*
* The USRFLG field will be at an offset of UDATAL1+1 from
* the beginning of the UDATAV field.
*
```

Examples

Appendix B. REXX RACVAR

The REXX RACVAR function is a RACF service for REXX execs; it provides information about the running user.

The REXX RACVAR function has four arguments. It provides information about:

USERID	The user ID that is in the ACEE
GROUP	The group name that is in the ACEE
SECLABEL	The seclabel that is in the ACEE
ACEESTAT	The status of the ACEE. The function returns NO ACEE, DEFAULT, DEFINED, or UNDEFINED

Below is a sample REXX exec that uses RACVAR to check the USERID, GROUP, and SECLABEL in the user's ACEE.

```
/* rexx */
say "Current ACEE status is " racvar('ACEESTAT') "."
if racvar('ACEESTAT') = 'NO ACEE' then
do
  say ' You have no ACEE defined'
end
else
do
  say "Your user ID is " racvar('USERID') "."
  say "You are connected to group " racvar('GROUP')"."
  current_seclabel = racvar('SECLABEL')
  if current_seclabel = ' ' then
  do
    say ' You have no SECLABEL defined'
  end
  else
  do
    say "Your SECLABEL is " current_seclabel"."
  end
end
end
return
```

To execute the REXX RACVAR function, your REXX parameter module must contain an entry for RACF's IRREFPCK directory package which, in turn, supports the RACVAR function. For descriptions on REXX parameter modules and updating and integrating them, see the *z/OS TSO/E REXX Reference* in the sections that describe Programming Services, Function Packages, and function directories.

Appendix C. IBM-supplied class descriptor table entries

NOT programming interface information

- DFTUACC
- GENLIST
- OPER
- POSIT
- RACLIST
- RACLREQ
- RVRSMAC
- SLBLREQ

End of NOT programming interface information

Table 231 lists the class entries supplied by IBM in the class descriptor table (ICHRRCDX). Other classes can be added to the class descriptor table (CDT) by your installation.

If you share a database between MVS and VM systems, you can use the VM classes in the CDT.

Table 231. Classes Supplied by IBM

Class

ACCTNUM	POSIT=126	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=39
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	OPER=NO	
		ID=46
	FIRST=ANY	
ACICSPCT	POSIT=5	OTHER=ANY
		MAXLNTH=13
		DFTUACC=NONE
	GROUP=BCICSPCT	
	OPER=NO	
		ID=37
	FIRST=ANY	

Table 231. Classes Supplied by IBM (continued)

Class		
AIMS	POSIT=4	OTHER=ALPHANUM
		MAXLNTH=8
		DFTUACC=NONE
	OPER=NO	
		ID=11
	FIRST=ALPHA	
ALCSAUTH	POSIT=548	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=62
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
	OPER=NO	
	PROFDEF=YES	ID=1
FIRST=ANY		
APPCLU	POSIT=118	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=35
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	OPER=NO	
		ID=57
FIRST=ALPHA		
APPCPORT	POSIT=87	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
		SLBLREQ=YES
		RVRSMAC=YES
	OPER=NO	
PROFDEF=YES	ID=98	
FIRST=ALPHA	MAXLENX=17	
APPCSERV	POSIT=84	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=73
	GENLIST=DISALLOWED	DFTRETC=8
	RACLREQ=YES	DFTUACC=NONE
		SLBLREQ=YES
	OPER=NO	
PROFDEF=YES	ID=105	
FIRST=ALPHANUM		

Table 231. Classes Supplied by IBM (continued)

Class		
APPSI	POSIT=88	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=26
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=READ
	OPER=NO	
	PROFDEF=YES	ID=97
	FIRST=ALPHANUM	
APPCTP	POSIT=89	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=82
	GENLIST=DISALLOWED	DFTRETC=8
	RACLREQ=YES	DFTUACC=NONE
		SLBLREQ=YES
	OPER=NO	
	PROFDEF=YES	ID=96
	FIRST=ALPHANUM	
APPL	POSIT=3	OTHER=ALPHANUM
	RACLIST=ALLOWED	MAXLNTH=8
	GENLIST=ALLOWED	
		DFTUACC=NONE
	OPER=NO	
		ID=8
	FIRST=ALPHA	
BCICSPCT	POSIT=5	OTHER=ANY
		MAXLNTH=13
		DFTUACC=NONE
	MEMBER=ACICSPCT	
	OPER=NO	
		ID=38
	FIRST=ANY	
CACHECLS	POSIT=569	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=16
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
		SLBLREQ=NO
	OPER=NO	
	PROFDEF=YES	ID=1
	FIRST=ALPHANUM	

Table 231. Classes Supplied by IBM (continued)

Class		
CBIND	POSIT=545	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=41
		DFTRETC=8
	OPER=NO	
		ID=1
	FIRST=ALPHANUM	
CCICSCMD	POSIT=5	OTHER=ANY
		MAXLNTH=21
		DFTUACC=NONE
	GROUP=VCICSCMD	
	OPER=NO	
		ID=52
	FIRST=ANY	
CIMS	POSIT=93	OTHER=ALPHANUM
	RACLIST=DISALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	GROUP=DIMS	
	OPER=NO	
		ID=88
FIRST=ALPHA		
CONSOLE	POSIT=107	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	DFTRETC=8
		DFTUACC=NONE
		RVRSMAC=YES
	OPER=NO	
		ID=68
FIRST=ANY		
CPSMOBJ	POSIT=57	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=44
	GENLIST=ALLOWED	
	GROUP=GCPSMOBJ	
	OPER=NO	
		ID=1
FIRST=ANY		

Table 231. Classes Supplied by IBM (continued)

Class		
CPSMXMP	POSIT=11	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=44
	OPER=NO	
		ID=1
	FIRST=ANY	
CSFKEYS	POSIT=98	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=73
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=YES	DFTUACC=NONE
	GROUP=GCSFKEYS	
	OPER=NO	
		ID=100
	FIRST=ALPHA	
CSFSERV	POSIT=98	OTHER=ALPHANUM
	RACLIST=ALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=YES	DFTUACC=NONE
	OPER=NO	
		ID=99
	FIRST=ALPHA	
DASDVOL	POSIT=0	OTHER=ALPHANUM
	RACLIST=ALLOWED	MAXLNTH=6
	GENLIST=ALLOWED	
	GROUP=GDASDVOL	
	OPER=YES	
		ID=5
	FIRST=ALPHANUM	
DBNFORM	POSIT=59	OTHER=ALPHANUM
	RACLIST=ALLOWED	MAXLNTH=8
		DFTUACC=NONE
	OPER=NO	
		ID=1
	FIRST=ALPHANUM	

Table 231. Classes Supplied by IBM (continued)

Class		
DCEUIDS	POSIT=544	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=73
	GENLIST=ALLOWED	DFTRETC=8
		DFTUACC=NONE
	OPER=NO	
		ID=1
	FIRST=ALPHANUM	
DCICSDCT	POSIT=5	OTHER=ANY
		MAXLNTH=13
		DFTUACC=NONE
	GROUP=ECICSDCT	
	OPER=NO	
		ID=31
	FIRST=ANY	
DEVICES	POSIT=115	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=39
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=YES	DFTUACC=NONE
		SLBLREQ=YES
	OPER=NO	
		ID=60
	FIRST=ANY	
DIGTCERT	POSIT=550	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
	OPER=NO	KEYQUAL=0
		ID=1
	FIRST=ANY	
DIGTCRIT	POSIT=563	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=YES	DFTUACC=NONE
	OPER=NO	KEYQUAL=0
		ID=1
	FIRST=ANY	

Table 231. Classes Supplied by IBM (continued)

Class		
DIGTMAP	POSIT=563	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=YES	DFTUACC=NONE
	OPER=NO	KEYQUAL=0
		ID=1
	FIRST=ANY	
DIGTRING	POSIT=550	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
	OPER=NO	KEYQUAL=0
		ID=1
	FIRST=ANY	
DIMS	POSIT=93	OTHER=ALPHANUM
	RACLIST=ALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	MEMBER=CIMS	
	OPER=NO	
		ID=89
	FIRST=ALPHA	
DIRACC	POSIT=71	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	DFTRETC=8
		DFTUACC=NONE
	OPER=NO	
	PROFDEF=NO	ID=107
	FIRST=ANY	
DIRAUTH	POSIT=105	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	DFTRETC=8
		DFTUACC=NONE
	OPER=NO	
	PROFDEF=NO	ID=70
	FIRST=ANY	

Table 231. Classes Supplied by IBM (continued)

Class			
DIRECTRY	POSIT=95	OTHER=ANY	
	RACLIST=DISALLOWED	MAXLNTH=153	
	GENLIST=DISALLOWED	DFTRETC=8	
		DFTUACC=NONE	
		SLBLREQ=YES	
	OPER=YES	KEYQUAL=2	
		ID=86	
	FIRST=ANY		
DIRSRCH	POSIT=70	OTHER=ANY	
	RACLIST=DISALLOWED	MAXLNTH=246	
	GENLIST=DISALLOWED	DFTRETC=8	
		DFTUACC=NONE	
	OPER=NO		
	PROFDEF=NO	ID=106	
	FIRST=ANY		
DLFCLASS	POSIT=92	OTHER=ANY	
	RACLIST=ALLOWED	MAXLNTH=64	
	GENLIST=DISALLOWED		
		DFTUACC=NONE	
	OPER=NO		
		ID=90	
	FIRST=ALPHA		
DSNADM	POSIT=539	OTHER=ANY	
	RACLIST=DISALLOWED	MAXLNTH=100	
	GENLIST=DISALLOWED	DFTRETC=4	
	RACLREQ=NO	DFTUACC=NONE	
		SLBLREQ=NO	
	OPER=NO		
	PROFDEF=YES	ID=1	
	FIRST=ANY		
DSNR	POSIT=7	OTHER=ANY	
	RACLIST=ALLOWED	MAXLNTH=39	
	GENLIST=DISALLOWED		
	OPER=NO		
		ID=18	
	FIRST=ALPHANUM		

Table 231. Classes Supplied by IBM (continued)

Class		
ECICSDCT	POSIT=5	OTHER=ANY
		MAXLNTH=13
		DFTUACC=NONE
	MEMBER=DCICSDCT	
	OPER=NO	
		ID=32
	FIRST=ANY	
EJBROLE	POSIT=568	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
	GROUP=GEJBROLE	SLBLREQ=NO
	OPER=NO	
	PROFDEF=YES	ID=1
FIRST=ANY	CASE=ASIS	
FACILITY	POSIT=8	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=39
	GENLIST=ALLOWED	
		DFTUACC=NONE
	OPER=NO	
		ID=19
	FIRST=ANY	
FCICSFCT	POSIT=5	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=17
		DFTUACC=NONE
	GROUP=HCICSFCT	
	OPER=NO	
		ID=27
	FIRST=ANY	
FIELD	POSIT=121	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=26
	GENLIST=ALLOWED	
		DFTUACC=NONE
	RACLREQ=YES	
	OPER=NO	
		ID=51
FIRST=ALPHA		

Table 231. Classes Supplied by IBM (continued)

Class		
FILE	POSIT=94	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=171
	GENLIST=DISALLOWED	DFTRETC=8
		DFTUACC=NONE
		SLBLREQ=YES
	OPER=YES	KEYQUAL=2
		ID=87
	FIRST=ANY	
FIMS	POSIT=101	OTHER=ALPHANUM
	RACLIST=DISALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	GROUP=HIMS	
	OPER=NO	
		ID=79
	FIRST=ALPHANUM	
FSOBJ	POSIT=72	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	DFTRETC=8
		DFTUACC=NONE
	OPER=NO	
	PROFDEF=NO	ID=108
	FIRST=ANY	
FSSEC	POSIT=73	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	DFTRETC=8
		DFTUACC=NONE
	OPER=NO	
	PROFDEF=NO	ID=109
	FIRST=ANY	
GCICSTRN	POSIT=5	OTHER=ANY
		MAXLNTH=13
		DFTUACC=NONE
	MEMBER=TCICSTRN	
	OPER=NO	
		ID=13
	FIRST=ANY	

Table 231. Classes Supplied by IBM (continued)

Class		
GCPSMOBJ	POSIT=57	OTHER=ANY
		MAXLNTH=246
	MEMBER=CPSMOBJ	
	OPER=NO	
		ID=1
	FIRST=ANY	
GCSFKEYS	POSIT=98	OTHER=NONATNUM
	RACLIST=DISALLOWED	MAXLNTH=17
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
	MEMBER=CSFKEYS	
	OPER=NO	
	ID=101	
	FIRST=NONATABC	
GDASDVOL	POSIT=0	OTHER=ALPHANUM
		MAXLNTH=6
	MEMBER=DASDVOL	
	OPER=YES	
		ID=39
	FIRST=ALPHANUM	
GDSNBP	POSIT=536	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
		SLBLREQ=NO
	MEMBER=MDSNBP	
	OPER=NO	
PROFDEF=YES	ID=1	
	FIRST=ANY	
GDSNCL	POSIT=538	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
		SLBLREQ=NO
	MEMBER=MDSNCL	
	OPER=NO	
PROFDEF=YES	ID=1	
	FIRST=ANY	

Table 231. Classes Supplied by IBM (continued)

Class		
GDSNDB	POSIT=528	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
		SLBLREQ=NO
	MEMBER=MDSNDB	
	OPER=NO	
	PROFDEF=YES	ID=1
	FIRST=ANY	
GDSNJR	POSIT=567	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
		SLBLREQ=NO
	MEMBER=MDSNJR	
	OPER=NO	
	PROFDEF=YES	ID=1
	FIRST=ANY	
GDSNPK	POSIT=534	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
		SLBLREQ=NO
	MEMBER=MDSNPK	
	OPER=NO	
	PROFDEF=YES	ID=1
	FIRST=ANY	
GDSNPN	POSIT=533	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
		SLBLREQ=NO
	MEMBER=MDSNPN	
	OPER=NO	
	PROFDEF=YES	ID=1
	FIRST=ANY	
GDSNSC	POSIT=562	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
		SLBLREQ=NO
	MEMBER=MDSNSC	
	OPER=NO	
	PROFDEF=YES	ID=1
	FIRST=ANY	

Table 231. Classes Supplied by IBM (continued)

Class		
GDSNSG	POSIT=537	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
		SLBLREQ=NO
	MEMBER=MDSNSG	
	OPER=NO	
	PROFDEF=YES	ID=1
	FIRST=ANY	
GDSNSM	POSIT=535	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
		SLBLREQ=NO
	MEMBER=MDSNSM	
	OPER=NO	
	PROFDEF=YES	ID=1
	FIRST=ANY	
GDSNSP	POSIT=561	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
		SLBLREQ=NO
	MEMBER=MDSNSP	
	OPER=NO	
	PROFDEF=YES	ID=1
	FIRST=ANY	
GDSNTB	POSIT=530	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
		SLBLREQ=NO
	MEMBER=MDSNTB	
	OPER=NO	
	PROFDEF=YES	ID=1
	FIRST=ANY	
GDSNTS	POSIT=529	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
		SLBLREQ=NO
	MEMBER=MDSNTS	
	OPER=NO	
	PROFDEF=YES	ID=1
	FIRST=ANY	

Table 231. Classes Supplied by IBM (continued)

Class			
GDSNUF	POSIT=560	OTHER=ANY	
	RACLIST=DISALLOWED	MAXLNTH=100	
	GENLIST=DISALLOWED	DFTRETC=4	
	RACLREQ=NO	DFTUACC=NONE	
		SLBLREQ=NO	
	MEMBER=MDSNUF		
	OPER=NO		
	PROFDEF=YES	ID=1	
	FIRST=ANY		
GDSNUT	POSIT=559	OTHER=ANY	
	RACLIST=DISALLOWED	MAXLNTH=100	
	GENLIST=DISALLOWED	DFTRETC=4	
	RACLREQ=NO	DFTUACC=NONE	
		SLBLREQ=NO	
	MEMBER=MDSNUT		
	OPER=NO		
	PROFDEF=YES	ID=1	
	FIRST=ANY		
GEJBROLE	POSIT=568	OTHER=ANY	
	RACLIST=DISALLOWED	MAXLNTH=246	
	GENLIST=DISALLOWED	DFTRETC=4	
	RACLREQ=NO	DFTUACC=NONE	
		SLBLREQ=NO	
	MEMBER=EJBROLE		
	OPER=NO		
	PROFDEF=YES	ID=1	
	FIRST=ANY	CASE=ASIS	
GIMS	POSIT=4	OTHER=ALPHANUM	
		MAXLNTH=8	
		DFTUACC=NONE	
	MEMBER=TIMS		
	OPER=NO		
		ID=10	
	FIRST=ALPHA		
	GINFOMAN	POSIT=85	OTHER=ANY
		RACLIST=DISALLOWED	MAXLNTH=44
GENLIST=DISALLOWED			
MEMBER=INFOMAN			
OPER=NO			
		ID=104	
	FIRST=ANY		

Table 231. Classes Supplied by IBM (continued)

Class		
GLOBAL	POSIT=6	OTHER=ANY
		MAXLNTH=8
		DFTUACC=NONE
	MEMBER=GMBR	
	OPER=NO	
		ID=17
	FIRST=ANY	
GMBR	POSIT=6	OTHER=ANY
		MAXLNTH=39
		DFTUACC=NONE
	GROUP=GLOBAL	
	OPER=NO	
		ID=16
	FIRST=ANY	
GMQADMIN	POSIT=80	OTHER=ANY
		MAXLNTH=62
		DFTRETC=8
		DFTUACC=NONE
	MEMBER=MQADMIN	
	OPER=NO	
		ID=121
FIRST=ANY		
GMQCHAN	POSIT=58	OTHER=ANY
		MAXLNTH=53
		DFTRETC=8
		DFTUACC=NONE
	MEMBER=MQCHAN	
	OPER=NO	
		ID=1
FIRST=ANY		
GMQNLIST	POSIT=79	OTHER=ANY
		MAXLNTH=53
		DFTRETC=8
		DFTUACC=NONE
	MEMBER=MQNLIST	
	OPER=NO	
		ID=119
FIRST=ANY		

Table 231. Classes Supplied by IBM (continued)

Class			
GMQPROC	POSIT=78	OTHER=ANY	
		MAXLNTH=53	
		DFTRETC=8	
		DFTUACC=NONE	
	MEMBER=MQPROC		
	OPER=NO		
		ID=117	
	FIRST=ANY		
	GMQQUEUE		
	POSIT=77	OTHER=ANY	
	MAXLNTH=53		
	DFTRETC=8		
	DFTUACC=NONE		
MEMBER=MQQUEUE			
OPER=NO			
	ID=4		
FIRST=ANY			
GSDSF	POSIT=100	OTHER=ANY	
		MAXLNTH=63	
		DFTUACC=NONE	
	MEMBER=SDSF		
	OPER=NO		
		ID=95	
	FIRST=ANY		
	GSOMDOBJ	POSIT=547	OTHER=ANY
			MAXLNTH=246
			DFTRETC=8
MEMBER=SOMDOBJ			
OPER=NO			
		ID=1	
FIRST=ALPHA			
GTERMINL		POSIT=2	OTHER=ALPHANUM
			MAXLNTH=8
		MEMBER=TERMINAL	
	OPER=NO		
		ID=42	
	FIRST=ALPHANUM		

Table 231. Classes Supplied by IBM (continued)

Class		
HCICSFCT	POSIT=5	OTHER=ANY
		MAXLNTH=17
		DFTUACC=NONE
	MEMBER=FCICSFCT	
	OPER=NO	
		ID=28
	FIRST=ANY	
HIMS	POSIT=101	OTHER=ALPHANUM
	RACLIST=DISALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	MEMBER=FIMS	
	OPER=NO	
		ID=80
FIRST=ALPHANUM		
IBMOPC	POSIT=60	OTHER=ANY
		MAXLNTH=60
		DFTUACC=NONE
	OPER=NO	
		ID=1
	FIRST=ALPHA	
ILMADMIN	POSIT=566	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=246
	GENLIST=ALLOWED	
		DFTUACC=NONE
		SLBLREQ=NONE
	OPER=NO	
		ID=1
FIRST=ANY		
INFOMAN	POSIT=85	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=44
	GENLIST=ALLOWED	
	GROUP=GINFOMAN	
	OPER=NO	
		ID=103
FIRST=ANY		

Table 231. Classes Supplied by IBM (continued)

Class		
IPCOBJ	POSIT=62	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	DFTRETC=8
		DFTUACC=NONE
	OPER=NO	
	PROFDEF=NO;	ID=1
FIRST=ANY		
JAVA	POSIT=556	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=246
		DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
	OPER=NO	
		ID=1
FIRST=ANY		
JCICSJCT	POSIT=5	OTHER=ANY
		MAXLNTH=17
		DFTUACC=NONE
	GROUP=KCICSJCT	
	OPER=NO	
		ID=29
FIRST=ANY		
JESINPUT	POSIT=108	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	DFTRETC=8
		DFTUACC=NONE
	OPER=NO	
		ID=67
FIRST=ANY		
JESJOBS	POSIT=109	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=39
	GENLIST=ALLOWED	DFTRETC=8
		DFTUACC=NONE
	OPER=NO	
		ID=66
FIRST=ANY		

Table 231. Classes Supplied by IBM (continued)

Class		
JESSPOOL	POSIT=110	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=53
	GENLIST=DISALLOWED	DFTRETC=8
		DFTUACC=NONE
	OPER=NO	
		ID=65
	FIRST=ANY	
KCICSJCT	POSIT=5	OTHER=ANY
		MAXLNTH=17
		DFTUACC=NONE
	MEMBER=JCICSJCT	
	OPER=NO	
	ID=30	
	FIRST=ANY	
KERBLINK	POSIT=565	OTHER=ANY
		MAXLNTH=240
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	RACLIST=DISALLOWED	
		DFTRETC=4
	OPER=NO	
	ID=1	
	FIRST=ANY	
KEYSMSTR	POSIT=543	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=39
	GENLIST=ALLOWED	DFTRETC=8
		DFTUACC=NONE
	OPER=NO	
		ID=1
	FIRST=ALPHANUM	
LDAPBIND	POSIT=571	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	OPER=NO	
		ID=1
	FIRST=ANY	

|
|
|
|
|
|
|
|
|
|

Table 231. Classes Supplied by IBM (continued)

Class		
LFSCCLASS	POSIT=12	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=246
		DFTUACC=NONE
	OPER=NO	
		ID=1
	FIRST=ALPHANUM	
LOGSTRM	POSIT=61	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=26
	GENLIST=ALLOWED	
		DFTUACC=NONE
	OPER=NO	
		ID=1
	FIRST=ANY	
MCICSPPT	POSIT=5	OTHER=ANY
		MAXLNTH=17
		DFTUACC=NONE
	GROUP=NCICSPPT	
	OPER=NO	
		ID=35
	FIRST=ANY	
MDSNBP	POSIT=536	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
	GROUP=GDSNBP	SLBLREQ=NO
	OPER=NO	
	PROFDEF=YES	ID=1
FIRST=ANY		
MDSNCL	POSIT=538	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
	GROUP=GDSNCL	SLBLREQ=NO
	OPER=NO	
	PROFDEF=YES	ID=1
FIRST=ANY		

Table 231. Classes Supplied by IBM (continued)

Class			
MDSNDB	POSIT=528	OTHER=ANY	
	RACLIST=DISALLOWED	MAXLNTH=100	
	GENLIST=DISALLOWED	DFTRETC=4	
	RACLREQ=NO	DFTUACC=NONE	
	GROUP=GDSNDB	SLBLREQ=NO	
	OPER=NO		
	PROFDEF=YES	ID=1	
	FIRST=ANY		
	MDSNJR	POSIT=567	OTHER=ANY
		RACLIST=DISALLOWED	MAXLNTH=100
GENLIST=DISALLOWED		DFTRETC=4	
RACLREQ=NO		DFTUACC=NONE	
GROUP=GDSNJR		SLBLREQ=NO	
OPER=NO			
PROFDEF=YES		ID=1	
FIRST=ANY			
MDSNPK		POSIT=534	OTHER=ANY
		RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4	
	RACLREQ=NO	DFTUACC=NONE	
	GROUP=GDSNPK	SLBLREQ=NO	
	OPER=NO		
	PROFDEF=YES	ID=1	
	FIRST=ANY		
	MDSNPN	POSIT=533	OTHER=ANY
		RACLIST=DISALLOWED	MAXLNTH=100
GENLIST=DISALLOWED		DFTRETC=4	
RACLREQ=NO		DFTUACC=NONE	
GROUP=GDSNPN		SLBLREQ=NO	
OPER=NO			
PROFDEF=YES		ID=1	
FIRST=ANY			
MDSNSC		POSIT=562	OTHER=ANY
		RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4	
	RACLREQ=NO	DFTUACC=NONE	
	GROUP=GDSNSC	SLBLREQ=NO	
	OPER=NO		
	PROFDEF=YES	ID=1	
	FIRST=ANY		

Table 231. Classes Supplied by IBM (continued)

Class			
MDSNSG	POSIT=537	OTHER=ANY	
	RACLIST=DISALLOWED	MAXLNTH=100	
	GENLIST=DISALLOWED	DFTRETC=4	
	RACLREQ=NO	DFTUACC=NONE	
	GROUP=GDSNSG	SLBLREQ=NO	
	OPER=NO		
	PROFDEF=YES	ID=1	
	FIRST=ANY		
	MDSNSM	POSIT=535	OTHER=ANY
		RACLIST=DISALLOWED	MAXLNTH=100
GENLIST=DISALLOWED		DFTRETC=4	
RACLREQ=NO		DFTUACC=NONE	
GROUP=GDSNSM		SLBLREQ=NO	
OPER=NO			
PROFDEF=YES		ID=1	
FIRST=ANY			
MDSNSP		POSIT=561	OTHER=ANY
		RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4	
	RACLREQ=NO	DFTUACC=NONE	
	GROUP=GDSNSP	SLBLREQ=NO	
	OPER=NO		
	PROFDEF=YES	ID=1	
	FIRST=ANY		
	MDSNTB	POSIT=530	OTHER=ANY
		RACLIST=DISALLOWED	MAXLNTH=100
GENLIST=DISALLOWED		DFTRETC=4	
RACLREQ=NO		DFTUACC=NONE	
GROUP=GDSNTB		SLBLREQ=NO	
OPER=NO			
PROFDEF=YES		ID=1	
FIRST=ANY			
MDSNTS		POSIT=529	OTHER=ANY
		RACLIST=DISALLOWED	MAXLNTH=100
	GENLIST=DISALLOWED	DFTRETC=4	
	RACLREQ=NO	DFTUACC=NONE	
	GROUP=GDSNTS	SLBLREQ=NO	
	OPER=NO		
	PROFDEF=YES	ID=1	
	FIRST=ANY		

Table 231. Classes Supplied by IBM (continued)

Class			
MDSNUF	POSIT=560	OTHER=ANY	
	RACLIST=DISALLOWED	MAXLNTH=100	
	GENLIST=DISALLOWED	DFTRETC=4	
	RACLREQ=NO	DFTUACC=NONE	
	GROUP=GDSNUF	SLBLREQ=NO	
	OPER=NO		
	PROFDEF=YES	ID=1	
	FIRST=ANY		
	MDSNUT	POSIT=559	OTHER=ANY
		RACLIST=DISALLOWED	MAXLNTH=100
GENLIST=DISALLOWED		DFTRETC=4	
RACLREQ=NO		DFTUACC=NONE	
GROUP=GDSNUT		SLBLREQ=NO	
OPER=NO			
PROFDEF=YES		ID=1	
FIRST=ANY			
MGMTCLAS		POSIT=123	OTHER=ALPHANUM
		RACLIST=ALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	DFTUACC=NONE	
	OPER=NO		
	ID=49		
	FIRST=ALPHA		
	MQADMIN	POSIT=80	OTHER=ANY
		MAXLNTH=62	
		DFTRETC=8	
		DFTUACC=NONE	
GROUP=GMQADMIN			
OPER=NO			
ID=120			
FIRST=ANY			
MQCHAN		POSIT=58	OTHER=ANY
		MAXLNTH=53	
	DFTRETC=8		
	DFTUACC=NONE		
	GROUP=GMQCHAN		
	OPER=NO		
	ID=1		
	FIRST=ANY		

Table 231. Classes Supplied by IBM (continued)

Class		
MQCMDS	POSIT=81	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=22
		DFTRETC=8
		DFTUACC=NONE
	OPER=NO	
		ID=122
	FIRST=ANY	
MQCONN	POSIT=82	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=10
		DFTRETC=8
		DFTUACC=NONE
	OPER=NO	
		ID=123
	FIRST=ANY	
MQNLIST	POSIT=79	OTHER=ANY
		MAXLNTH=53
		DFTRETC=8
		DFTUACC=NONE
	GROUP=GMQNLIST	
	OPER=NO	
		ID=118
	FIRST=ANY	
MQPROC	POSIT=78	OTHER=ANY
		MAXLNTH=53
		DFTRETC=8
		DFTUACC=NONE
	GROUP=GMQPROC	
	OPER=NO	
		ID=116
	FIRST=ANY	
MQQUEUE	POSIT=77	OTHER=ANY
		MAXLNTH=53
		DFTRETC=8
		DFTUACC=NONE
	GROUP=GMQQUEUE	
	OPER=NO	
		ID=2
	FIRST=ANY	

Table 231. Classes Supplied by IBM (continued)

Class		
NCICSPPT	POSIT=5	OTHER=ANY
		MAXLNTH=17
		DFTUACC=NONE
	MEMBER=MCICSPPT	
	OPER=NO	
		ID=36
	FIRST=ANY	
NDSLINK	POSIT=554	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	OPER=NO	PROFDEF=YES
	DFTRETC=4	ID=1
	FIRST=ANY	
NETCMDS	POSIT=68	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=246
		ID=1
	FIRST=ALPHA	
NETSPAN	POSIT=67	OTHER=ANY
		MAXLNTH=8
		ID=1
	FIRST=ALPHA	
NODES	POSIT=103	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=24
	GENLIST=DISALLOWED	
	RACLREQ=YES	DFTUACC=NONE
	MEMBER=NODMBR	
	OPER=NO	
		ID=72
FIRST=ANY		

Table 231. Classes Supplied by IBM (continued)

Class		
NODMBR	POSIT=103	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	GROUP=NODES	
	OPER=NO	
		ID=43
	FIRST=ANY	
NOTELINK	POSIT=553	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=64
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	OPER=NO	PROFDEF=YES
	DFTRETC=4	ID=1
	FIRST=ANY	
NVASAPDT	POSIT=97	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=17
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	OPER=NO	
		ID=83
	FIRST=ANY	
OIMS	POSIT=101	OTHER=ALPHANUM
	RACLIST=DISALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	GROUP=WIMS	
	OPER=NO	
		ID=81
	FIRST=ALPHANUM	
OPERCMD5	POSIT=112	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=39
	GENLIST=DISALLOWED	
	RACLREQ=YES	DFTUACC=NONE
	OPER=NO	
		ID=63
	FIRST=ANY	

Table 231. Classes Supplied by IBM (continued)

Class		
PCICSPSB	POSIT=5	OTHER=ANY
		MAXLNTH=17
		DFTUACC=NONE
	GROUP=QCICSPSB	
	OPER=NO	
		ID=14
	FIRST=ANY	
PERFGRP	POSIT=125	OTHER=NUMERIC
	RACLIST=ALLOWED	MAXLNTH=3
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	OPER=NO	
		ID=47
	FIRST=NUMERIC	
PIMS	POSIT=101	OTHER=ALPHANUM
	RACLIST=DISALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	GROUP=QIMS	
	OPER=NO	
		ID=75
FIRST=ALPHANUM		
PMBR	POSIT=13	OTHER=ALPHANUM
		MAXLNTH=44
		DFTUACC=NONE
	GROUP=PROGRAM	
	OPER=NO	
		ID=40
	FIRST=ALPHA	
PRINTSRV	POSIT=570	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=17
	GENLIST=ALLOWED	
		DFTUACC=NONE
	OPER=NO	
		ID=1
	FIRST=ANY	

Table 231. Classes Supplied by IBM (continued)

Class		
PROCACT	POSIT=75	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	DFTRETC=8
		DFTUACC=NONE
	OPER=NO	
	PROFDEF=NO	ID=111
	FIRST=ANY	
PROCESS	POSIT=74	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	DFTRETC=8
		DFTUACC=NONE
	OPER=NO	
	PROFDEF=NO	ID=110
	FIRST=ANY	
PROGRAM	POSIT=13	OTHER=ALPHANUM
		MAXLNTH=8
		DFTUACC=NONE
	MEMBER=PMBR	
	OPER=NO	
		ID=41
	FIRST=ALPHA	
PROPCNTL	POSIT=119	OTHER=ALPHANUM
	RACLIST=ALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	
	RACLREQ=YES	DFTUACC=NONE
	OPER=NO	
		ID=56
	FIRST=ALPHANUM	
PSFMPL	POSIT=113	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=39
	GENLIST=DISALLOWED	DFTRETC=8
	RACLREQ=YES	DFTUACC=NONE
	OPER=YES	
		ID=62
	FIRST=ANY	

Table 231. Classes Supplied by IBM (continued)

Class		
PTKTDATA	POSIT=76	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=39
	RACLREQ=YES	DFTUACC=NONE
	OPER=NO	
		ID=112
	FIRST=ALPHANUM	
PTKTVAL	POSIT=76	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=39
	OPER=NO	
		ID=1
	FIRST=ANY	
QCICSPSB	POSIT=5	OTHER=ANY
		MAXLNTH=17
		DFTUACC=NONE
	MEMBER=PCICSPSB	
	OPER=NO	
		ID=15
QIMS	POSIT=101	OTHER=ALPHANUM
	RACLIST=DISALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	MEMBER=PIMS	
	OPER=NO	
	ID=76	
	FIRST=ALPHANUM	
RACGLIST	POSIT=10	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=14
	GENLIST=DISALLOWED	DFTRC=4
	RACLREQ=NO	DFTUACC=NONE
		SLBLREQ=NO
	OPER=NO	
	PROFDEF=YES	ID=1
	FIRST=ANY	

Table 231. Classes Supplied by IBM (continued)

Class			
RACFVARS	POSIT=102	OTHER=ALPHANUM	
	RACLIST=ALLOWED	MAXLNTH=8	
	GENLIST=DISALLOWED	DFTRETC=4	
	RACLREQ=YES	DFTUACC=NONE	
	MEMBER=RVARSMBR		
	OPER=NO		
	ID=74		
	FIRST=ANY		
	REALM	POSIT=564	OTHER=ANY
		MAXLNTH=240	
GENLIST=DISALLOWED			
DFTUACC=NONE			
RACLIST=ALLOWED			
DFTRETC=4			
OPER=NO			
ID=1			
RMTOPS	POSIT=86	OTHER=ANY	
	MAXLNTH=246		
	DFTUACC=NONE		
	OPER=NO		
	ID=102		
	FIRST=ALPHA		
	RODMMGR	POSIT=69	OTHER=ANY
		MAXLNTH=8	
ID=113			
FIRST=ALPHANUM			
ROLE		POSIT=551	OTHER=ANY
		RACLIST=DISALLOWED	MAXLNTH=246
		GENLIST=DISALLOWED	DFTRETC=8
		PROFDEF=YES	DFTUACC=NONE
	OPER=NO		
	ID=1		
	FIRST=ANY		

Table 231. Classes Supplied by IBM (continued)

Class		
RRSFDATA	POSIT=65	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=246
	GENLIST=ALLOWED	DFTRETC=4
	RACLREQ=NO	DFTUACC=NONE
	OPER=NO	KEYQUAL=0
		ID=1
	FIRST=ANY	
RVARSMBR	POSIT=102	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=39
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	GROUP=RACFVARS	
	OPER=NO	
		ID=73
	FIRST=ANY	
SCDMBR	POSIT=9	OTHER=ANY
		MAXLNTH=39
		DFTUACC=NONE
	GROUP=SECDATA	
	OPER=NO	
		ID=25
	FIRST=ANY	
SCICSTST	POSIT=5	OTHER=ANY
		MAXLNTH=17
		DFTUACC=NONE
	GROUP=UCICSTST	
	OPER=NO	
		ID=33
	FIRST=ANY	MAXLENX=25
SDSF	POSIT=100	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=63
	GENLIST=ALLOWED	
		DFTUACC=NONE
	GROUP=GSDSF	
	OPER=NO	
		ID=94
	FIRST=ANY	

Table 231. Classes Supplied by IBM (continued)

Class		
SECDATA	POSIT=9	OTHER=ALPHA
		MAXLNTH=8
		DFTUACC=NONE
	MEMBER=SCDMBR	
	OPER=NO	
		ID=26
	FIRST=ALPHA	
SECLABEL	POSIT=117	OTHER=ALPHANUM
	RACLIST=ALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	DFTRETC=8
	RACLREQ=YES	DFTUACC=NONE
	OPER=NO	
		ID=58
	FIRST=ALPHA	
SERVAUTH	POSIT=558	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=64
		DFTRETC=4
	RACLREQ=YES	DFTUACC=NONE
	OPER=NO	
		ID=1
	FIRST=ALPHA	
SFSCMD	POSIT=99	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	DFTRETC=8
		DFTUACC=NONE
	OPER=NO	
		ID=93
	FIRST=ANY	
SERVER	POSIT=546	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=41
		DFTRETC=8
	OPER=NO	
		ID=1
	FIRST=ALPHANUM	

Table 231. Classes Supplied by IBM (continued)

Class		
SIMS	POSIT=101	OTHER=ALPHANUM
	RACLIST=DISALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	GROUP=UIMS	
	OPER=NO	
		ID=77
	FIRST=ALPHANUM	
SMESSAGE	POSIT=116	OTHER=ALPHANUM
	RACLIST=ALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	DFTRETC=0
		DFTUACC=NONE
	OPER=NO	
		ID=59
	FIRST=ALPHANUM	
	SOMDOBJ	POSIT=547
RACLIST=ALLOWED		MAXLNTH=246
		DFTRETC=8
GROUP=GSOMDOBJ		
OPER=NO		
		ID=1
FIRST=ALPHANUM		
STARTED		POSIT=66
	RACLIST=ALLOWED	MAXLNTH=17
	GENLIST=DISALLOWED	
	RACLREQ=YES	DFTUACC=NONE
	OPER=NO	
		ID=1
	FIRST=ALPHA	
	STORCLAS	POSIT=122
RACLIST=ALLOWED		MAXLNTH=8
GENLIST=DISALLOWED		
		DFTUACC=NONE
OPER=NO		
		ID=50
FIRST=ALPHA		

Table 231. Classes Supplied by IBM (continued)

Class		
SUBSYSNM	POSIT=83	OTHER=ALPHANUM
	RACLIST=ALLOWED	MAXLNTH=8
		DFTUACC=NONE
	OPER=NO	
		ID=1
	FIRST=ALPHA	
SURROGAT	POSIT=104	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=17
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	OPER=NO	
		ID=71
	FIRST=ANY	
SYSMVIEW	POSIT=542	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=52
	GENLIST=DISALLOWED	
	RACLREQ=YES	DFTUACC=NONE
	OPER=NO	
		ID=1
	FIRST=ALPHANUM	
TAPEVOL	POSIT=1	OTHER=ALPHANUM
		MAXLNTH=6
		SLBLREQ=YES
	OPER=YES	
		ID=6
	FIRST=ALPHANUM	
TCICSTRN	POSIT=5	OTHER=ANY
		MAXLNTH=13
		DFTUACC=NONE
	GROUP=GCICSTRN	
	OPER=NO	
	ID=12	
	FIRST=ANY	

Table 231. Classes Supplied by IBM (continued)

Class		
TEMPDSN	POSIT=106	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=39
	GENLIST=DISALLOWED	DFTRETC=8
		DFTUACC=NONE
	OPER=NO	
	PROFDEF=NO	ID=69
	FIRST=ANY	
TERMINAL	POSIT=2	OTHER=ALPHANUM
	RACLIST=ALLOWED	MAXLNTH=8
	GENLIST=ALLOWED	
	GROUP=GTERMINL	SLBLREQ=YES
		RVRSMAC=YES
	OPER=NO	
		ID=7
	FIRST=ALPHANUM	
TIMS	POSIT=4	OTHER=ALPHANUM
		MAXLNTH=8
		DFTUACC=NONE
	GROUP=GIMS	
	OPER=NO	
		ID=9
	FIRST=ALPHANUM	
TMEADMIN	POSIT=549	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=246
	GENLIST=ALLOWED	DFTRETC=8
		DFTUACC=NONE
	OPER=NO	
		ID=1
	FIRST=ALPHANUM	
TSOAUTH	POSIT=124	OTHER=ALPHANUM
	RACLIST=ALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	OPER=NO	
		ID=48
	FIRST=ALPHANUM	

Table 231. Classes Supplied by IBM (continued)

Class		
TSOPROC	POSIT=127	OTHER=ALPHANUM
	RACLIST=ALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	OPER=NO	
		ID=45
	FIRST=ALPHA	
UCICSTST	POSIT=5	OTHER=ANY
		MAXLNTH=17
		DFTUACC=NONE
	MEMBER=SCICSTST	
	OPER=NO	
		ID=34
	FIRST=ANY	MAXLENX=25
UIMS	POSIT=101	OTHER=ALPHANUM
	RACLIST=DISALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	MEMBER=SIMS	
	OPER=NO	
		ID=78
	FIRST=ALPHANUM	
UNIXMAP	POSIT=552	OTHER=NUMERIC
	RACLIST=DISALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	DFTRETC=4
		DFTUACC=NONE
	OPER=NO	
		ID=1
	FIRST=ALPHA	
UNIXPRIV	POSIT=555	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	DFTRETC=4
		DFTUACC=NONE
	RACLREQ=YES	SLBLREQ=NO
	OPER=NO	
		ID=1
	FIRST=ANY	

Table 231. Classes Supplied by IBM (continued)

Class		
VCICSCMD	POSIT=5	OTHER=ANY
		MAXLNTH=21
		DFTUACC=NONE
	MEMBER=CCICSCMD	
	OPER=NO	
		ID=53
	FIRST=ANY	
VMBATCH	POSIT=15	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=8
	GENLIST=ALLOWED	DFTRETC=4
		DFTUACC=NONE
		ID=24
	FIRST=ANY	
VMBR	POSIT=120	OTHER=ALPHANUM
	RACLIST=DISALLOWED	MAXLNTH=39
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	GROUP=VMEVENT	
	OPER=NO	
		ID=54
	FIRST=ALPHA	
VMCMD	POSIT=14	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=17
	GENLIST=ALLOWED	DFTRETC=4
		DFTUACC=NONE
		ID=22
	FIRST=ANY	
VMEVENT	POSIT=120	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=16
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	MEMBER=VMBR	
	OPER=NO	
		ID=55
	FIRST=ALPHA	

Table 231. Classes Supplied by IBM (continued)

Class		
VMMAC	POSIT=91	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	DFTRETC=8
		DFTUACC=NONE
		SLBLREQ=YES
	OPER=NO	
	PROFDEF=NO	ID=91
	FIRST=ANY	
VMMDISK	POSIT=18	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=22
	GENLIST=ALLOWED	
		DFTUACC=NONE
		ID=20
	FIRST=ANY	
VMNODE	POSIT=16	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=8
	GENLIST=ALLOWED	
		DFTUACC=NONE
		ID=23
	FIRST=ANY	
VMPOSIX	POSIT=63	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=246
	GENLIST=DISALLOWED	DFTRETC=4
		DFTUACC=NONE
	OPER=NO	
		ID=1
	FIRST=ANY	
VMRDR	POSIT=17	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=17
	GENLIST=ALLOWED	DFTRETC=4
		DFTUACC=NONE
		ID=21
	FIRST=ANY	

Table 231. Classes Supplied by IBM (continued)

Class		
VMSEGMT	POSIT=90	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=246
	GENLIST=ALLOWED	DFTRETC=4
		DFTUACC=NONE
		SLBLREQ=YES
	OPER=NO	
		ID=92
	FIRST=ANY	
VMXEVENT	POSIT=96	OTHER=ANY
	RACLIST=DISALLOWED	MAXLNTH=16
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	MEMBER=VMXMBR	
	OPER=NO	
		ID=85
	FIRST=ALPHA	
VTAMAPPL	POSIT=114	OTHER=ALPHANUM
	RACLIST=ALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	
	RACLREQ=YES	DFTUACC=NONE
	OPER=NO	
		ID=61
		FIRST=ALPHANUM
VMXMBR	POSIT=96	OTHER=ALPHANUM
	RACLIST=DISALLOWED	MAXLNTH=39
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	GROUP=VMXEVENT	
	OPER=NO	
		ID=84
	FIRST=ALPHA	
WIMS	POSIT=101	OTHER=ALPHANUM
	RACLIST=DISALLOWED	MAXLNTH=8
	GENLIST=DISALLOWED	
		DFTUACC=NONE
	MEMBER=OIMS	
	OPER=NO	
		ID=82
	FIRST=ALPHANUM	

Table 231. Classes Supplied by IBM (continued)

Class		
WRITER	POSIT=111	OTHER=ANY
	RACLIST=ALLOWED	MAXLNTH=39
	GENLIST=DISALLOWED	DFTRETC=8
		DFTUACC=NONE
		SLBLREQ=YES
		RVRSMAC=YES
	OPER=NO	
		ID=64
	FIRST=ANY	

Appendix D. RACF database templates

Included in this appendix are the following templates:

1. GROUP
2. USER
3. CONNECT
4. DATA SET
5. GENERAL
6. RESERVED

Attention

Do not modify the RACF database templates (SYS1.MODGEN(IRRTEMP1)). Such modification is not supported by IBM and may result in damage to your RACF database or other unpredictable results.

Segment Fields:

1. The first field in a segment of a template cannot be retrieved or updated. This field has a Field ID of 001 and is usually described in the '**Field Being Described**' column as 'Start of segment fields'.
2. The TME segment fields are intended to be updated by Tivoli applications, which manage updates, permissions, and cross references among the fields. The TME fields should only be directly updated on an exception basis. See *z/OS Security Server RACF Command Language Reference* for formats of the field data as enforced by the RACF commands. Use caution when directly updating TME fields, as the updates may be overridden by subsequent actions of Tivoli applications.

Format of field definitions

The RACF database templates contain a definition for each field in the profile.

Each field definition contains information about the field in the following format:

Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value Type
-----------------------------------	-------------	--------	--------	----------------------------	--------------------

Field Name	Character data.
Field ID	Reference number.
Flag 1 field	The bits have the following meanings when they are turned on:
Bit 0:	The field is a member of a repeat group.
Bit 1:	The definition describes a combination field.
Bit 2:	The field is a flag byte.
Bit 3:	The field contains the count of members in the repeat group following this field.
Bit 4:	The definition describes a combination field continued in next entry.
Bit 5:	The field (for example, PASSWORD) is masked.
Bit 6:	The field is sorted in ascending order.
Bit 7:	The field is a statistical field. A value is always stored for this field, even when it is equal to the defined null value for the field.

Database templates

Flag 2		The bits have the following meanings when they are turned on:
	Bit 0:	Changes to this field affect security and cause ACEEs to be purged from VLF.
	Bit 1:	The field is padded on the left with binary zeros when values shorter than the field length are retrieved.
	Bit 2:	This field represents a 3-byte date field.
	Bit 3:	This field is an Application Identity Mapping alias name.
	Bit 4:	This field is not to be unloaded by the Database Unload utility (IRRDBU00).
	Bits 5-7:	Reserved for IBM's use.
Field Length		Field length on return from ICHEINTY or RACROUTE REQUEST=EXTRACT (0 is variable length).
Default Value		Field default. If the field is not present in the profile, this byte is propagated throughout the returned field as the default value.
Type		Data type of each field. In this column, character is represented as 'Char', integer is represented as 'Int', and binary is represented as 'Bin'. 'Date' and 'Time' are also possible data types.

The type of a combination field that represents a single field is the same as that single field. There is no "type" associated with a combination field which represents multiple fields.

Repeat groups on the RACF database

A repeat group consists of one or more sequential fields within a profile that are able to be repeated within that profile. A field that belongs to a repeat group is only defined once in the template, but can be repeated as many times as necessary within the actual profile. A count field precedes the repeat group in the profile indicating how many of these groups follow.

If a field in a profile has a fixed length, a value (less than 255) in the field definition within the template specifies its actual length. If a field in a profile has a variable length, the value in the field definition is 0. In both cases, the actual field length is contained in the physical data mapped by the field definition.

Data field types

RACF stores information in the RACF database in many different formats. This section identifies the major data types that RACF stores. Exceptions and additional detail can be found in the description of each specific field within the templates.

Date fields

The format of the 3-byte date fields is *yydddF*, which represents a packed decimal number in which *y* represents year, *d* represents day, and *F* represents the sign. Examples of RACF date values are X'98111C' and X'94099D'.

The format of the 4-byte date fields should be *yyyymmdd*, which represents a packed decimal number in which *y* represents year, *m* represents month, and *d* represents day. Examples of RACF date values are X'19980421' and X'19940409'.

RACF might use any of the following values for null dates: X'FFFFFF', X'00000D', X'00000C', and X'000000' for 3-byte addresses, and X'FFFFFFF', X'0000000D', X'0000000C', and X'00000000' for 4-byte addresses. However, you should always set null dates to either X'00000F' for 3-byte addresses and X'0000000F' for 4-byte addresses.

Time fields

The format for the 4-byte time fields are *hhmmssstc* where *h* represents hours, *m* represents minutes, *s* represents seconds, *t* represents tenths of seconds, and *c* represents hundredths of seconds. There is no sign byte. For information on the 8-byte version, see the TIME macro as documented in *z/OS MVS Programming: Assembler Services Reference IAR-XCT*.

Integer fields

Integers are stored as unsigned binary values. These values can be 1, 2, or 4 bytes in length.

Character fields

Character fields are padded with blanks to the right.

Combination fields on the RACF database

The database templates also contain definitions called *combination fields*.

Combination fields do not describe a field of a profile. They contain the field numbers that identify the respective field definitions. You can use a combination as an alias to access multiple fields with one ICHEACTN or RACROUTE REQUEST=EXTRACT macro. For more information, see "Example 2: Adding a user ID to a data set access list" on page 343.

In addition, you can use the combination field to provide aliases for individual fields.

The format of a combination field definition is different from a non-combination definition. Its format is as follows:

Field Name	Character data.
Field ID	Reference number.
Flag 1	The hex representation of the flag bits for this field. For combination fields, bit 1 is on. For a continuation of combination fields, bit 4 is also on.
Flag 2	The hex representation of the flag bits for this field. For combination fields, all bits are off.
Combination IDs	If nonzero, combination IDs represent the position of a non-combination field within the template segment. There can be up to 5 field IDs representing the template fields that comprise this combination field.
Type	Data type of each field. In this column, character is represented as 'Char', integer is represented as 'Int', and binary is represented as 'Bin'. 'Date' and 'Time' are also possible data types.
Comments	Comment field.

Determining space requirements for the profiles

The formula for calculating the space required for each segment (Base RACF information, TSO, DFP, and so on) of each profile in the RACF database is as follows:

$$P = 20 + L + F1 + F4 + R$$

Where:

- P** = The number of bytes required for a profile segment
L = The number of bytes in the profile name

Database templates

- F1** = The sum of the lengths of all fields that contain data and have a length of 1 to 127 bytes, plus 2 bytes for every field counted.
- For example, if a segment contains 3 non-null fields of length 8, $F1 = (3 * 8) + (3 * 2) = 24 + 6 = 30$.
- F4** = The sum of the lengths of all fields that contain data and have a length of 128 to $2^{**}31$ bytes, plus 5 bytes for every field counted.
- For example, if a segment contains a non-null field 150 bytes long and a non-null field 255 bytes long, $F4 = 150 + 255 + (2 * 5) = 150 + 255 + 10 = 415$
- R** = The sum of the lengths of all repeat groups. If a repeat group has no occurrences, then it has a length of 0 bytes. If a repeat group has 1 or more occurrences, then the length of each repeat group is calculated as follows:

$$9 + N + G1 + G4$$

- N** = The number of occurrences of the group
- G1** = The sum of the lengths of all fields in the group, which have a length of 1 to 127 bytes, plus 1 byte for every field counted. If a field has a length of zero, it will still take up 1 byte in the profile.
- G4** = The sum of the lengths of all fields in the group, which have a length of 128 to $2^{**}31$ bytes, plus 4 bytes for every field counted.

For example, consider a group with two occurrences. Each occurrence contains an 8-byte field and a variable length field. In the first occurrence, the variable length field is 30 bytes and in second occurrence, it is 200 bytes. The length of the group is:

$$9 + 2 + G1 + G4$$

G1 is $(8 + 1) + (30 + 1)$ from the first occurrence and $(8 + 1)$ from the second, for a total of 49 bytes. G4 is $(200 + 4)$ from the second occurrence, or 204 bytes. So, the length of the group is $9 + 2 + 49 + 204$, or 264 bytes.

Note: For each repeat group (except CGGRPCT in the USER profile), the amount of data may not exceed 65535 bytes to ensure proper processing by programs retrieving the data using ICHEINTY with DATAMAP=OLD. To calculate the amount of data to determine whether it will fit within this limit, examine the template definitions for the repeat group and the data for that repeat group contained within the profile. For each fixed length field in each occurrence of the repeat group add the length of the field as shown in its template definition. For each variable length field in each occurrence of the repeat group add the length of the data in the field plus one. When you are done, the total cannot exceed 65535.

For example, this would translate into a maximum of 8191 group connections per user, based on the CONGRPCT repeat group in the USER template. This group contains one 8-byte field, making the calculation of the limit a simple one of dividing 65535 by 8 and dropping any remainder.

As another example, this would translate into a maximum of 5957 users connected to a group, based on the ACLCNT repeat group in the GROUP template. This group contains one 8-byte field (USERID), one 1-byte field (USERACS), and one 2-byte field (ACSCNT). This gives a total length of eleven for the fixed-length fields in each occurrence. Dividing 65535 by 11 and dropping the remainder gives the limit of 5957.

When calculating F1 and F4, remember that statistical fields (Flag1/bit 7 on, in the template definition) are always stored in a profile segment, even when the field contains a null value. For example, LJTIME will always add 3 bytes to the length of a USER profile Base segment, regardless of whether it contains a zero value or some other value. Other fields will only exist in the segment if a specific value has been added for that field.

Note: The RACF database space required for a segment is a multiple of the 256-byte slots required to contain the segment. For example, if a USER profile Base segment contains 188 bytes of data, it will still require 256 bytes of space in the RACF database.

Determining space requirements for alias index entries

An exact formula for calculating the space required for alias entries cannot be derived due to index block compression, and the mechanics of the higher level index blocks. The following is an approximate formula for space taken up in the alias index block sequence set (level 1) by an index entry:

$$AIE = 16 + (N * (2 + BPL)) + AKL$$

Where:

- AIE** = Alias index entry length
- N** = The number of base profile names. Most aliases are only allowed 1 base profile association.
- BPL** = Base profile name length. The base profile is named in the alias index entry. Because the base profile is a user or group profile, valid BPL values are between 1 and 8.
- AKL** = Alias index entry, key length. The first 3 bytes are template number, segment number, and field number. Additional bytes of the alias index key are taken up by the alias value. These lengths vary according to each alias field.

Group template for the RACF database

The group template describes the fields of group profiles in the RACF database.

NOT programming interface information	
ACSCNT	FLDNAME
FIELD	FLDVALUE
FLDCNT	INITCNT
FLDFLAG	
End of NOT programming interface information	

Notes:

- Application developers should not depend on being able to use RACROUTE REQUEST=EXTRACT for the BASE segment fields on any security product other than RACF. These products are expected to support only such segments as DFP and TSO.
- The TME segment fields are intended to be updated by the Tivoli applications, which manage updates, permissions, and cross references among the fields. The TME fields should only be directly updated on an exception basis. See *z/OS Security Server RACF Command Language Reference* for formats of the

Group Template

field data as enforced by the RACF commands. Use caution when directly updating TME fields, as the updates might be overridden by subsequent actions of Tivoli applications.

The contents of the group template are as follows:

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
The following is the BASE segment of the GROUP template.							
GROUP	001	00	00	00000000	00		
ENTYPE	002	00	00	00000001	01	Int	The number (1) corresponding to group profiles.
VERSION	003	00	00	00000001	01	Int	The version field from the profile. Always X'01'.
SUPGROUP	004	00	80	00000008	FF	Char	The superior group to this group.
AUTHDATE	005	00	20	00000003	FF	Date	The date the group was created.
AUTHOR	006	00	80	00000008	FF	Char	The owner (user ID or group name) of the group.
INITCNT	007	00	00	00000002	FF		Reserved for IBM's use.
UACC	008	20	00	00000001	00	Bin	The universal group authority. (The authority of a user to the group if the user is not connected to the group.)
							Bit Meaning When Set 0 JOIN authority 1 CONNECT authority 2 CREATE authority 3 USE authority 4-7 Reserved for IBM's use Note: This field has a value of X'00', except for group VSAMDSET, where the value is X'20'.
NOTRMUAC	009	20	00	00000001	00	Bin	If bit 0 is on, the user must be specifically authorized (by the PERMIT command) to use the terminal. If off, RACF uses the terminal's UACC.
INSTDATA	010	00	00	00000000	00	Char	Installation data.
MODELNAM	011	00	00	00000000	00	Char	Data set model profile name. The profile name begins with the second qualifier; the high-level qualifier is not stored.
FLDCNT	012	10	00	00000004	00		Reserved for IBM's use.
FLDNAME	013	80	00	00000008	00		Reserved for IBM's use.
FLDVALUE	014	80	00	00000000	00		Reserved for IBM's use.
FLDFLAG	015	A0	00	00000001	00		Reserved for IBM's use.
SUBGRPCT	016	10	00	00000004	00	Int	The number of subgroups of the group.
SUBGRPNM	017	80	80	00000008	00	Char	A list of the subgroup names.
ACLCNT	018	10	00	00000004	00	Int	The number of users connected to the group.
USERID	019	80	00	00000008	00	Char	The user ID of each user connected to the group.
USERACS	020	A0	00	00000001	00	Bin	The group authority of each user connected to the group.
							Bit Meaning When Set 0 JOIN authority 1 CONNECT authority 2 CREATE authority 3 USE authority 4-7 Reserved for IBM's use
ACSCNT	021	80	00	00000002	00		Reserved for IBM's use.

Group Template

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
USRCNT	022	10	00	00000004	00	Int	Reserved for installation's use. See Note 1 .
USRNM	023	80	00	00000008	00		Reserved for installation's use. See Note 1 .
USRDATA	024	80	00	00000000	00		Reserved for installation's use. See Note 1 .
USRFLG	025	A0	00	00000001	00		Reserved for installation's use. See Note 1 .
UNVFLG	026	20	00	00000001	00	Bin	Identifies the group as having (bit 0 is on) or not having the UNIVERSAL attribute.

Note 1: Intended usage for these fields is to allow the installation to store additional data in this profile. USRNM should have a field name to use as a key to identify each unique occurrence of a row in the repeat group. USRDATA and USRFLG hold the data associated with that name. For more information, see "Example 5: Updating the installation fields" on page 346.

Field Name	Field ID	Flag 1	Flag 2	Combination Field IDs				Type		
The following are the COMBINATION fields.										
DEFDATE	000	40	00	005	000	000	000	000	Char	Alias for AUTHDATE
CREADATE	000	40	00	005	000	000	000	000	Char	Alias for AUTHDATE
OWNER	000	40	00	006	000	000	000	000	Char	Alias for AUTHOR
FIELD	000	40	00	013	014	015	000	000		FLDNAME, FLDVALUE, and FLDFLAG
ACL	000	40	00	019	020	021	000	000		USERID, USERACS, and ACSCNT
USERDATA	000	40	00	023	024	025	000	000		USRNM, USERDATA, and USERFLG

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
The following is the DFP Segment of the GROUP Template.							
DFP	001	00	00	00000000	00		Start of segment
DATAAPPL	002	00	00	00000000	00	Char	Data Application
DATACLAS	003	00	00	00000000	00	Char	Data Class
MGMTCLAS	004	00	00	00000000	00	Char	Management Class
STORCLAS	005	00	00	00000000	00	Char	Storage Class
The following is the OMVS Segment of the GROUP Template.							
OMVS	001	00	00	00000000	00		Start of segment
GID	002	00	10	00000004	FF	Int	GID
The following is the OVM Segment of the GROUP Template.							
OVM	001	00	00	00000000	00		Start of segment
GID	002	00	00	00000004	FF	Int	GID
The following is the TME Segment of the GROUP Template.							
TME	001	00	00	00000000	00		Start of segment fields
ROLEN	002	10	00	00000004	00	Int	Count of roles
ROLES	003	80	00	00000000	00	Char	Role names

User template for the RACF database

The user template describes the fields of the user profiles in a RACF database.

NOT programming interface information

CATEGORY	ENCTYPE	FLDVALUE	PREVKEY
CONGRPCT	FIELD	MAGSTRIP	PREVKEYV
CONGRPNM	FLDCNT	NUMCTGY	PWDCNT
CURKEY	FLDFLAG	OLDPWD	PWDGEN
CURKEYV	FLDNAME	OLDPWDNM	SALT

User Template

End of NOT programming interface information

Note: Application developers should not depend on being able to use RACROUTE REQUEST=EXTRACT for the BASE segment fields on any security product other than RACF. These products are expected to support only such segments as DFP and TSO.

The contents of the user template (base segment) are as follows:

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
The following is the BASE segment of the USER template.							
USER	001	00	00	00000000	00		
ENTYPE	002	00	00	00000001	02	Int	The number (2) corresponding to user profiles.
VERSION	003	00	00	00000001	01	Int	The version field from the profile. Always X'01'.
AUTHDATE	004	00	20	00000003	FF	Date	The date the user was defined to RACF.
AUTHOR	005	00	00	00000008	FF	Char	The owner (user ID or group name) of the user profile.
FLAG1	006	20	80	00000001	00	Bin	Identifies the user as having (bit 0 is on) or not having the ADSP attribute.
FLAG2	007	20	80	00000001	00	Bin	Identifies the user as having (bit 0 is on) or not having the SPECIAL attribute.
FLAG3	008	20	80	00000001	00	Bin	Identifies the user as having (bit 0 is on) or not having the OPERATIONS attribute.
FLAG4	009	20	80	00000001	00	Bin	Identifies the user as having (bit 0 is on) or not having the REVOKE attribute.
FLAG5	010	20	80	00000001	00	Bin	Identifies the user as having (bit 0 is on) or not having the GRPACC attribute.
PASSINT	011	00	80	00000001	FF	Int	The interval in days (represented by a number between 1 and 254) that the user's password is in effect. If it is X'FF', the user's password never expires. See the description of the SETR PASSWORD(INTERVAL...) processing instructions in <i>z/OS Security Server RACF Command Language Reference</i> for more details.
PASSWORD	012	04	80	00000008	FF	Char	The password associated with the user. For masking, the masked password is stored. For DES, the encrypted user ID is stored. If the installation provides its own password authentication, data returned by the ICHDEX01 exit is stored.
PASSDATE	013	00	20	00000003	FF	Date	The date the password was last changed.
PGMRNAME	014	00	00	00000020	FF	Char	The name of the user.
DFLTGRP	015	00	00	00000008	FF	Char	The default group associated with the user. A value of X'FF' indicates that no group was specified.
LJTIME	016	01	00	00000004	FF	Time	The time that the user last entered the system by using RACROUTE REQUEST=VERIFY.
LJDATE	017	01	20	00000003	FF	Date	The date that the user last entered the system by using RACROUTE REQUEST=VERIFY.
INSTDATA	018	00	80	00000000	00	Char	Installation data.

User Template

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
UAUDIT	019	20	80	00000001	00	Bin	Identifies whether all RACROUTE REQUEST=AUTH, RACROUTE REQUEST=DEFINE, (and, if the caller requests logging, RACROUTE REQUEST=FASTAUTH) macros issued for the user and all RACF commands (except SEARCH, LISTDSD, LISTGRP, LISTUSER, and RLIST) issued by the user will be logged. If bit 0 is on, they are logged. If bit 0 is off, logging might still occur for other reasons, as identified in <i>z/OS Security Server RACF Auditor's Guide</i> .
FLAG6	020	20	80	00000001	00	Bin	Identifies the user as having (bit 0 is on) or not having the AUDITOR attribute.
FLAG7	021	20	80	00000001	00	Bin	If bit 0 is on, and FLAG8 has bit 0 on, an operator identification card (OID card) is needed to enter the system.
FLAG8	022	20	80	00000001	00	Bin	If bit 1 is on, this is a protected user ID, which cannot enter the system by any means requiring a password or OID card. If bit 0 is on, an operator identification card (OID card) is required when logging on to the system.
MAGSTRIP	023	04	00	00000000	00	Bin	The operator identification associated with the user from the masked or encrypted OID card data required to authenticate this user, as supplied by a supported 327x (such as 3270 and 3278) OID card reader.
PWDGEN	024	00	00	00000001	FF	Int	Current password generation number.
PWDCNT	025	10	00	00000004	00	Int	Number of old passwords present.
OLDPWDNM	026	80	00	00000001	00	Int	Generation number of previous password.
OLDPWD	027	84	00	00000008	FF	Char	Previous password. This is an encrypted password value.
REVOKECT	028	01	80	00000001	FF	Int	Count of unsuccessful password attempts. Note: You can use ALTER when setting this field, but you cannot use ALTERI.
MODELNAM	029	00	80	00000000	00	Char	Data set model profile name. The profile name begins with the second qualifier; the high-level qualifier is not stored.
SECLEVEL	030	00	80	00000001	FF	Int	The number that corresponds to the user's security level. For more information on security levels, see <i>z/OS Security Server RACF Security Administrator's Guide</i> .
NUMCTGY	031	10	80	00000004	00	Int	Number of security categories.
CATEGORY	032	80	80	00000002	00	Int	A number that corresponds to the security categories to which the user has access.
REVOKEDT	033	00	20	00000000	00	Date	The date the user will be revoked. This field either has length 0, or contains a 3-byte revoke date.
RESUMEDT	034	00	20	00000000	00	Date	The date the user will be resumed. This field either has length 0, or contains a 3-byte resume date.
LOGDAYS	035	20	00	00000001	00	Bin	The days of the week the user cannot log on (Bit 0 of this field equals Sunday, bit 1 equals Monday, and so on).

User Template

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
LOGTIME	036	00	80	00000000	00	Time	The time of the day the user can log on. If present (length of variable field not equal to 0), it is specified as 6 bytes formatted as two 3-byte packed decimal fields, <i>0ssssC0eeeeC</i> , where <i>ssss</i> represents the start time (<i>hhmm</i>) from the ALU...WHEN(TIMES(...)) specification and <i>eeee</i> represents the end time. For <i>hhmm</i> , <i>hh</i> represents hours, and <i>mm</i> represents minutes.
FLDCNT	037	10	00	00000004	00		Reserved for IBM's use.
FLDNAME	038	80	00	00000008	00		Reserved for IBM's use.
FLDVALUE	039	80	00	00000000	00		Reserved for IBM's use.
FLDFLAG	040	A0	00	00000001	00		Reserved for IBM's use.
CLCNT	041	10	80	00000004	00	Int	The number of classes in which the user is allowed to define profiles.
CLNAME	042	80	80	00000008	00	Char	A class in which the user is allowed to define profiles. (The user has the CLAUTH attribute.) The user can also define profiles in any other classes with POSIT values matching these classes.
CONGRPCT	043	10	80	00000004	00	Int	The number of groups that the user is connected to.
CONGRPNM	044	80	80	00000008	00	Char	A group that the user is connected to.
USRCNT	045	10	00	00000004	00	Int	Reserved for installation's use. Note: Intended usage: For installation to store additional data in this profile. USRNM should have a field name to use as a key to identify each unique occurrence of a row in the repeat group. USRDATA and USRFLG hold the data associated with that name. For more information, see "Example 5: Updating the installation fields" on page 346.
USRNM	046	80	80	00000008	00		
USRDATA	047	80	80	00000000	00		
USRFLG	048	A0	80	00000001	00		
SECLABEL	049	00	80	00000008	00	Char	Security label.
CGGRPCT	050	10	80	00000004	00	Int	Number of Connect Group entries. Information from the following CGxxx fields is also available through the logical connect profiles (ICHEINTY with CLASS=CONNECT) in the database. See "Connect template for the RACF database" on page 407 for more details.
CGGRPNM	051	82	80	00000008	00	Char	Connect Group Entry Name.
CGAUTHDA	052	80	A0	00000003	FF	Date	Date the user was connected.
CGAUTHOR	053	80	80	00000008	FF	Char	Owner of connect occurrence.
CGLJTIME	054	81	00	00000004	FF	Time	Time of RACROUTE REQUEST=VERIFY.
CGLJDATE	055	81	20	00000003	FF	Date	Date of RACROUTE REQUEST=VERIFY.
CGUACC	056	A0	80	00000001	00	Bin	Default universal access.
CGINITCT	057	81	00	00000002	FF	Int	Number of RACROUTE REQUEST=VERIFY requests that were successfully processed where the value specified in the CGRPNM field was the current connect group.
CGFLAG1	058	A0	80	00000001	00	Bin	If bit 0 is on, the user has the ADSP attribute in that group.
CGFLAG2	059	A0	80	00000001	00	Bin	If bit 0 is on, the user has the SPECIAL attribute in that group.
CGFLAG3	060	A0	80	00000001	00	Bin	If bit 0 is on, the user has the OPERATIONS attribute in that group.

User Template

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
CGFLAG4	061	A0	80	00000001	00	Bin	If bit 0 is on, the user has the REVOKE attribute in that group.
CGFLAG5	062	A0	80	00000001	00	Bin	If bit 0 is on, the user has the GRPACC attribute in that group.
CGNOTUAC	063	A0	80	00000001	00	Bin	If bit 0 is on, the user must be specifically authorized (by the PERMIT command) to use a terminal. If off, RACF uses the terminal's UACC.
CGGRPAUD	064	A0	80	00000001	00	Bin	If bit 0 is on, the user has the GROUP AUDITOR attribute in that group.
CGREVKDT	065	80	20	00000000	00	Date	The date the user will be revoked. This field either has length 0, or contains a 3-byte revoke date.
CGRESMDT	066	80	20	00000000	00	Date	The date the user will be resumed. This field either has length 0, or contains a 3-byte resume date.
TUCNT	067	10	00	00000002	00	Int	Number of user ID associations.
TUKEY	068	80	00	00000016	00	Char	Associated node and user ID.
TUDATA	069	80	00	00000000		Bin	<p>Byte Meaning When Set</p> <p>0-7 The associated node name.</p> <p>8-15 The associated user ID.</p> <p>Associated user ID association data</p> <p>Byte Meaning When Set</p> <p>0 Version number of the TUDATA entry.</p> <p>1 Bitstring</p> <p>0 Specifies the user as having (bit is on) or not having (bit is off) a peer user ID association.</p> <p>1 Specifies the user as being (bit is on) the manager of a managed user ID association.</p> <p>2 Specifies the user as being (bit is on) managed by a managed user ID association.</p> <p>3 An association request for this user is pending (bit is on) on a remote RRSF node.</p> <p>4 An association request for this user is pending (bit is on) on the local RRSF node.</p> <p>5 Specifies that password synchronization is in effect (bit is on) for this peer-user ID association.</p> <p>6 Specifies that the association request for this user was rejected (bit is on).</p> <p>7 Reserved for IBM's use.</p> <p>2-20 Reserved for IBM's use.</p> <p>21-24 The date the user ID association was defined. (yyyymmdd)</p>

User Template

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
						Time	25-32 The time the user ID association was defined. For the format of the time, see the TIME macro as documented in <i>z/OS MVS Programming: Assembler Services Reference IAR-XCT</i> .
						Char	32-36 The date the user ID association was approved or refused. (yyyymmdd)
						Int	37-44 The time the user ID association was approved or refused. For the format of the time, see the TIME macro as documented in <i>z/OS MVS Programming: Assembler Services Reference IAR-XCT</i> .
						Char	45-56 Reserved for IBM's use.
							57-64 The user ID that created the entry. Number of certificate names. Name of certificate. Names correspond to profiles in the DIGTCERT class for the user. Label associated with the certificate. Subject's distinguished name. Public key associated with the certificate. Reserved for IBM's use. Restricted Access = BIT0. Number of DIGTNMAP Mapping Profiles that specify this user ID. Label associated with this mapping. Name of mapping profile. The names correspond to profiles in the DIGTNMAP Class.
CERTCT	070	10	00	00000004	00		
CERTNAME	071	80	00	00000000	00		
CERTLABL	072	80	00	00000000	00		
CERTSJDN	073	80	00	00000000	00		
CERTPUBK	074	80	00	00000000	00		
CERTRSV3	075	80	00	00000000	00		
FLAG9	076	20	80	00000001	00		
NMAPCT	077	10	00	00000004	00		
NMAPLABL	078	80	00	00000000	00		
NMAPNAME	079	80	00	00000000	00		
NMAPRSV1	080	80	00	00000000	00		Reserved.
NMAPRSV2	081	80	00	00000000	00		Reserved.
NMAPRSV3	082	80	00	00000000	00		Reserved.
NMAPRSV4	083	80	00	00000000	00		Reserved.
NMAPRSV5	084	80	00	00000000	00		Reserved.

Field Name Field ID Flag 1 Flag 2 Combination Field IDs Type

Following are the COMBINATION fields of the USER template

DEFDATE	000	40	00	004	000	000	000	000	
CREADATE	000	40	00	004	000	000	000	000	
OWNER	000	40	00	005	000	000	000	000	
PASSDATA	000	40	00	012	013	000	000	000	
NAME	000	40	00	014	000	000	000	000	
OLDPSWDS	000	40	00	026	027	000	000	000	
LOGINFO	000	40	00	035	036	000	000	000	
FIELD	000	40	00	038	039	040	000	000	
USERDATA	000	40	00	046	047	048	000	000	
CGDEFDAT	000	40	00	052	000	000	000	000	

Combination.
Fields.

User Template

Field Name	Field ID	Flag 1	Flag 2	Combination Field IDs				Type
CGCREADT	000	40	00	052	000	000	000	000
CGOWNER	000	40	00	053	000	000	000	000
TUENTRY	000	40	00	068	069	000	000	000
CERTLIST	000	40	00	071	072	000	000	000
CERTLST2	000	40	00	071	072	073	074	000
CERTLST3	000	40	00	071	072	073	000	000
CERTSIGL	000	40	00	071	073	074	000	000

Template

Field Name (Character Data)

Following is the DFP segment of the USER template

Field Name	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
DFP	001	00	00	00000000	00		Start of segment fields
DATAAPPL	002	00	00	00000000	00	Char	Data Application; maximum length=8
DATACLAS	003	00	00	00000000	00	Char	Data Class; maximum length=8
MGMTCLAS	004	00	00	00000000	00	Char	Management Class; maximum length=8
STORCLAS	005	00	00	00000000	00	Char	Storage Class; maximum length=8

Following is the TSO segment of the USER template

TSO	001	00	00	00000000	00		Start of segment fields
TACCNT	002	00	00	00000000	00	Char	Default account numbers; maximum length=40
TCOMMAND	003	00	00	00000000	00	Char	Default command at logon; maximum length=80
TDEST	004	00	00	00000000	00	Char	Destination identifier; maximum length=8
THCLASS	005	00	00	00000000	00	Char	Default hold class; maximum length=1
TJCLASS	006	00	00	00000000	00	Char	Default job class
TLPROC	007	00	00	00000000	00	Char	Default logon procedure; maximum length=8
TLSIZE	008	00	00	00000004	00	Int	Logon size
TMCLASS	009	00	00	00000000	00	Char	Default message class; maximum length=1
TMSIZE	010	00	00	00000004	00	Int	Maximum region size
TOPTION	011	20	00	00000001	00	Bin	Default for mail notices and OIDcard
TPERFORM	012	00	00	00000004	00	Int	Performance group
TRBA	013	00	00	00000003	00	Bin	RBA of user's broadcast area
TSCLASS	014	00	00	00000000	00	Char	Default sysout class
TUDATA	015	00	00	00000002	00	Bin	2 bytes of hex user data
TUNIT	016	00	00	00000000	00	Char	Default unit name; maximum length=8
TUPT	017	00	00	00000000	00	Bin	Data from UPT control block
TSOSLABL	018	00	00	00000000	00	Char	Default logon SECLABEL; maximum length=8
TCONS	019	00	00	00000000	00	Char	Consoles support

Following is the CICS segment of the USER template

CICS	001	00	00	00000000	00		Start of segment fields
OPIDENT	002	00	00	00000003	00	Char	Operator identification; 1 to 3 bytes in length
OPCLASSN	003	10	00	00000004	00	Int	Count of operator class values
OPCLASS	004	80	00	00000001	00	Int	Operator class
OPPRTY	005	00	40	00000002	00	Int	Operator priority
XRFSOFF	006	20	00	00000001	00	Bin	XRF Re-signon option: <ul style="list-style-type: none"> • Bit 0 on = FORCE • Bit 0 off = NOFORCE

User Template

Template
Field Name
(Character
Data)

Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type
TIMEOUT	00	40	00000002	00	Bin

Field Being Described

Terminal time-out value

Notes:

Two 1-byte binary fields:

1. first one = hours (0-99)
2. second one = minutes (0-59)
3. special case: hours=0, minutes=60
treated the same as hours=1,
minutes=0

Following is the LANGUAGE segment of the USER template

LANGUAGE	001	00	00	00000000	00	
USERNL1	002	00	80	00000003	00	Char
USERNL2	003	00	80	00000003	00	Char

Start of segment fields

User's primary language; 3-character code returned by the MVS message service. For more information, see *z/OS MVS Programming: Assembler Services Guide*.
User's secondary language

Following is the OPERPARM segment of the USER template

OPERPARM	001	00	00	00000000	00	
OPERSTOR	002	00	00	00000002	00	Bin
OPERAUTH	003	00	00	00000002	00	Bin
OPERMFRM	004	00	00	00000002	00	Bin
OPERLEVL	005	00	00	00000002	00	Bin
OPERMON	006	00	00	00000002	00	Bin
OPERROUT	007	00	00	00000000	00	Bin
OPERLOGC	008	00	00	00000001	00	Bin

Start of segment fields

STORAGE keyword

AUTH keyword:

- X'8000' = MASTER
- X'4000' = ALL
- X'2000' = SYS
- X'10000' = IO
- X'0800' = CONS
- X'0400' = INFO

MFORM keyword:

- Bit 0 indicates T
- Bit 1 indicates S
- Bit 2 indicates J
- Bit 3 indicates M
- Bit 4 indicates X

LEVEL keyword:

- Bit 0 indicates R
- Bit 1 indicates I
- Bit 2 indicates CE
- Bit 3 indicates E
- Bit 4 indicates IN
- Bit 5 indicates NB
- Bit 6 indicates ALL

Bit 6 is mutually exclusive with all other bits except Bit 5.

MONITOR keyword:

- Bit 0 indicates JOB NAMES
- Bit 1 indicates JOB NAME ST
- Bit 2 indicates SESS
- Bit 3 indicates SESST
- Bit 4 indicates STATUS

Bits 0 and 1 are mutually-exclusive, as are bits 2 and 3.

ROUTCODE keyword; 16-bit length bitstring in which each bit indicates a particular ROUTCODE.

LOGCMDRESP keyword.

Value Meaning When Set

X'80' Indicates SYSTEM was specified.

X'40' Indicates NO was specified.

User Template

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
OPERMGID	009	00	00	00000001	00	Bin	MIGID keyword. Value Meaning When Set X'80' Indicates YES was specified. X'40' Indicates NO was specified.
OPERDOM	010	00	00	00000001	00	Bin	DOM keyword. Value Meaning When Set X'80' Indicates NORMAL was specified. X'40' Indicates ALL was specified. X'20' Indicates NONE was specified.
OPERKEY	011	00	00	00000000	00	Bin	KEY keyword; maximum length=8
OPERCMD5	012	00	00	00000000	00	Bin	CMDSYS keyword; maximum length=8 (or **)
OPERUD	013	00	00	00000001	00	Bin	UD keyword. Value Meaning When Set X'80' Indicates YES was specified. X'40' Indicates NO was specified.
OPERM CNT	014	10	00	00000004	00	Bin	Count of MSCOPE systems
OPERM SCP	015	80	00	00000008	00	Bin	MSCOPE systems
OPERALTG	016	00	00	00000000	00	Bin	ALTGRP keyword Value Meaning When Set X'80' Indicates YES was specified. X'40' Indicates NO was specified.
OPERAUTO	017	00	00	00000001	00	Bin	AUTO keyword; X'80' indicates YES; X'40' indicates NO.
Following is the WORK ATTRIBUTES segment of the USER template							
WORKATTR	001	00	80	00000000	00		Start of segment fields
WANAME	002	00	80	00000000	00	Char	User name for SYSOUT; maximum length=60
WABLDG	003	00	80	00000000	00	Char	Building for delivery; maximum length=60
WADEPT	004	00	80	00000000	00	Char	Department for delivery; maximum length=60
WAROOM	005	00	80	00000000	00	Char	Room for delivery; maximum length=60
WAADDR1	006	00	80	00000000	00	Char	SYSOUT address line 1; maximum length=60
WAADDR2	007	00	80	00000000	00	Char	SYSOUT address line 2; maximum length=60
WAADDR3	008	00	80	00000000	00	Char	SYSOUT address line 3; maximum length=60
WAADDR4	009	00	80	00000000	00	Char	SYSOUT address line 4; maximum length=60
WAACCNT	010	00	80	00000000	00	Char	Account number; maximum length=255
Following is the OMVS segment of the USER template							
OMVS	001	00	00	00000000	00		Start of segment fields
UID	002	00	10	00000004	FF	Int	UID
HOME	004	00	00	00000000	00	Char	HOME Path; maximum length=1023
PROGRAM	005	00	00	00000000	00	Char	Initial Program; maximum length=1023
CPUTIME	006	00	00	00000004	FF	Int	CPUTIMEMAX
ASSIZE	007	00	00	00000004	FF	Int	ASSIZEMAX
FILEPROC	008	00	00	00000004	FF	Int	FILEPROCMAX
PROCUSER	009	00	00	00000004	FF	Int	PROCUSERMAX
THREADS	010	00	00	00000004	FF	Int	THREADSMAX
MMAPAREA	011	00	00	00000004	FF	Int	MMAPAREAMAX
Following is the NETVIEW segment of the USER template							
NETVIEW	001	00	00	00000000	00		Start of segment fields

User Template

Template

Field Name (Character Data)

Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
IC	002	00	00	00000000	00	Char	The command or command list to be processed by NetView for this operator when the operator logs on to Netview; maximum length=255.
CONSNAME	003	00	00	00000000	00	Char	The default MCS console identifier; maximum length=8.
CTL	004	20	00	00000001	00	Bin	CTL keyword - Specifies whether a security check is performed for this NetView operator when they try to use a span or try to do a cross-domain logon. Value Meaning When Set X'00' Indicates CTL was not specified or CTL(SPECIFIC) was specified. X'80' Indicates CTL(GLOBAL) was specified. X'40' Indicates CTL(GENERAL) was specified.
MSGRECVR	005	20	00	00000001	00	Bin	MSGRECVR keyword Value Meaning When Set X'00' Indicates the operator can receive unsolicited messages that are not routed to a specific NetView operator. X'80' Indicates the operator cannot receive unsolicited messages that are not routed to a specific NetView operator.
OPCLASSN	006	10	00	00000004	00	Int	Count of operator class values.
OPCLASS	007	80	40	00000002	00	Int	Specifies a NetView scope class for which the operator has authority. This is a 2-byte repeating field. Each member can have fixed-binary values from 1 to 2040.
DOMAINSN	008	10	00	00000004	00	Int	The number of domains the NetView operator controls.
DOMAINS	009	80	00	00000000	00	Char	Specifies the identifier of NetView programs in another NetView domain for which this operator has authority. This is a variable length (5-character maximum) repeating field.
NGMFADMN	010	20	00	00000001	00	Bin	NGMFADMN keyword Value Meaning When Set X'00' The NetView operator does not have administrator authority to the NetView Graphic Monitor Facility (NGMF). X'80' The NetView operator has administrator authority to the NetView graphic monitor facility (NGMF).
NGMFVSPN	011	00	00	00000000	00		NetView Graphic Monitor Facility view span options; maximum length=8
Following is the DCE segment of the USER template							
DCE	001	00	00	00000000	00		Start of segment fields
UUID	002	00	00	00000036	FF	Char	User's DCE principal's UUID; exactly 36 characters, in the format <i>nnnnnnnnn-nnnn-nnnn-nnnn-nnnnnnnnnnnnn</i> where <i>n</i> is any hexadecimal digit.

User Template

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
DCENAME	003	00	00	00000000	00	Char	User's DCE principal name; maximum length=1023
HOMECELL	004	00	00	00000000	00	Char	Home cell for this DCE user; maximum length=1023, and it must start with either /.../ or /:./
HOMEUUID	005	00	00	00000036	FF	Char	Home cell UUID; exactly 36 characters, in the format nnnnnnnn-nnnn-nnnn-nnnn-nnnnnnnnnnn where n is any hexadecimal digit.
DCEFLAGS	006	20	00	00000001	00	Bin	User flags
DPASSWDS	007	00	00	00000000	00	Char	Current DCE password
DCEENCRY	008	00	00	00000071	00	Bin	PW mask/enrypt key
Following is the OVM segment of the USER template							
OVMS	001	00	00	00000000	00		Start of segment fields
UID	002	00	00	00000004	FF	Int	OVMS - UID
HOME	003	00	00	00000000	00	Char	Home path; maximum length=1023
PROGRAM	004	00	00	00000000	00	Char	Initial program; maximum length=1023
FSROOT	005	00	00	00000000	00	Char	File system root; maximum length=1023
Following is the LNOTES segment of the USER template							
LNOTES	001	00	00	00000000	00		Start of segment fields
SNAME	002	00	10	00000000	00	Char	User's short name; maximum length=64
Following is the NDS segment of the USER template							
NDS	001	00	00	00000000	00		Start of segment fields
UNAME	002	00	10	00000000	00	Char	User's user name; maximum length=246
Following is the KERB segment of the USER template							
KERB	001	00	00	00000000	00		Start of segment fields
KERBNAME	002	00	00	00000000	00	Char	Kerberos principal name
MINTKTLF	003	00	00	00000000	00	Char	Reserved
MAXTKTLF	004	00	00	00000000	00	Char	Maximum ticket life
DEFTKTLF	005	00	00	00000000	00	Char	Reserved
SALT	006	00	00	00000000	00	Char	Current key salt
ENCTYPE	007	00	00	00000000	00	Char	Encryption type
CURKEYV	008	00	00	00000000	00	Char	Current key version
CURKEY	009	00	00	00000000	00	Char	Current DES key
PREVKEYV	010	00	00	00000000	00	Char	Previous key version
PREVKEY	011	00	00	00000000	00	Char	Previous DES key
ENCRYPT	012	00	00	00000004	55	Bin	Encryption types for SETROPTS KERBLVL(1)
Following is the PROXY segment of the USER template							
PROXY	001	00	00	00000000	00		Start of segment fields
LDAPHOST	002	00	00	00000000	00	Char	LDAP server URL; maximum length: 1023
BINDDN	003	00	00	00000000	00	Char	Bind distinguished name; maximum length: 1023
BINDPW	004	00	08	00000000	00	Char	Bind password; maximum length: 128
BINDPWKY	005	00	08	00000071	00	Char	Bind password mask or encrypt key
Following is the EIM segment of the USER template							
LDAPPROF	1	00	00	00000000	00	Char	LDAPBIND profile name

Connect template for the RACF database

The connect template is included to maintain compatibility with previous releases. You can continue to code macros to manipulate CONNECT data. This template is provided to show what fields continue to be supported. Information that was formerly stored in CONNECT profiles was moved to the USER profile. The information is in the CGGRPCT repeat group, and the fields are prefixed by "CG".

Connect Template

Notes:

1. Application developers should not depend on being able to use RACROUTE REQUEST=EXTRACT for the BASE segment fields on any security product other than RACF. These products are expected to support only such segments as DFP and TSO.
2. The default values for this template are located in the User Template.

The contents of the connect template are as follows:

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
CONNECT	001	00	00	00000000			
ENTYPE	002	00	00	00000001		Int	The number (3) corresponding to connect profiles.
VERSION	003	00	00	00000001		Int	The version field from the profile. Always X'01'.
AUTHDATE	004	00	A0	00000003		Date	The date the user was connected to the group.
AUTHOR	005	00	80	00000008		Char	The owner (user ID) of the connect entry.
LJTIME	006	01	00	00000004		Time	The time that RACROUTE REQUEST=VERIFY was last issued for this user and group.
LJDATE	007	01	20	00000003		Date	The date that RACROUTE REQUEST=VERIFY was last issued for this user and group.
UACC	008	20	80	00000001		Bin	The default universal access authority assigned to the user for this group.
							Bit Meaning When Set 0 ALTER access 1 CONTROL access 2 UPDATE access 3 READ access 4 EXECUTE access 5-6 Reserved for IBM's use 7 EXECUTE access
INITCNT	009	01	00	00000002		Int	The number of RACROUTE REQUEST=VERIFY macro instructions issued for this user and group.
FLAG1	010	20	80	00000001		Bin	Identifies the user as having (bit 0 is on) or not having the ADSP attribute.
FLAG2	011	20	80	00000001		Bin	Identifies the user as having (bit 0 is on) or not having the group-SPECIAL attribute.
FLAG3	012	20	80	00000001		Bin	Identifies the user as having (bit 0 is on) or not having the group-OPERATIONS attribute.
FLAG4	013	20	80	00000001		Bin	Identifies the user as having (bit 0 is on) or not having the REVOKE attribute.
FLAG5	014	20	80	00000001		Bin	Identifies the user as having (bit 0 is on) or not having the GRPACC attribute.
NOTRMUAC	015	20	80	00000001		Bin	Identifies whether the user must be authorized by the PERMIT command with at least READ authority to access a terminal. (If not, RACF uses the terminal's universal access authority.) If bit 0 is on, the user must be specifically authorized to use the terminal.
GRPAUDIT	016	20	80	00000001		Bin	Identifies the user as having (bit 0 is on) or not having the group-AUDITOR attribute.

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
REVOKEDT	017	00	20	00000000		Date	The date the user will be revoked. This field either has length 0, or contains a 3-byte revoke date.
RESUMEDT	018	00	20	00000000		Date	The date the user will be resumed. This field either has length 0, or contains a 3-byte resume date.

Field Name	Field ID	Flag 1	Flag 2	Combination Field IDs	Type
The following are the COMBINATION fields.					
DEFDATE	000	40	00	004 000 000 000 000	Char
CREADATE	000	40	00	004 000 000 000 000	Char
OWNER	000	40	00	005 000 000 000 000	Char

Data set template for the RACF database

The data set template describes the fields of the data set profiles in a RACF database.

NOT programming interface information			
ACL2VAR	CATEGORY	FLDFLAG	FLDVALUE
AUDITQF	FIELD	FLDNAME	NUMCTGY
AUDITQS	FLDCNT		
End of NOT programming interface information			

Notes:

1. Application developers should not depend on being able to use RACROUTE REQUEST=EXTRACT for the BASE segment fields on any security product other than RACF. These products are expected to support only such segments as DFP and TSO.
2. The TME segment fields are intended to be updated by Tivoli applications, which manage updates, permissions, and cross references among the fields. The TME fields should only be directly updated on an exception basis. See *z/OS Security Server RACF Command Language Reference* for formats of the field data as enforced by the RACF commands. Use caution when directly updating TME fields, as the updates may be overridden by subsequent actions of Tivoli applications.

The contents of the data set template are as follows:

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
DATASET	001	00	00	00000000	00		
ENTYPE	002	00	00	00000001	04	Int	The number (4) corresponding to data set profiles.
VERSION	003	00	00	00000001	01	Int	The version field from the profile. Always X'01'.
CREADATE	004	00	20	00000003	FF	Date	The date the data set was initially defined to RACF; 3-byte date.
AUTHOR	005	00	00	00000008	FF	Char	The owner of the data set.

Data Set Template

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
LREFDAT	006	01	20	00000003	FF	Date	The date the data set was last referenced; 3-byte date.
LCHGDAT	007	01	20	00000003	FF	Date	The date the data set was last updated; 3-byte date.
ACSALTR	008	01	00	00000002	FF	Int	The number of times the data set was accessed with ALTER authority.
ACSCNTL	009	01	00	00000002	FF	Int	The number of times the data set was accessed with CONTROL authority.
ACSUPDT	010	01	00	00000002	FF	Int	The number of times the data set was accessed with UPDATE authority.
ACSREAD	011	01	00	00000002	FF	Int	The number of times the data set was accessed with READ authority.
UNIVACS	012	20	00	00000001	00	Bin	The universal access authority for the data set.
							Bit Meaning When Set 0 ALTER access 1 CONTROL access 2 UPDATE access 3 READ access 4 EXECUTE access 5-6 Reserved for IBM's use 7 EXECUTE access
FLAG1	013	20	00	00000001	00	Bin	Identifies whether the data set is a group data set. If bit 0 is on, the data set is a group data set.
AUDIT	014	20	00	00000001	00	Bin	Audit Flags.
							Bit Meaning When Set 0 Audit all accesses 1 Audit successful accesses 2 Audit accesses that fail 3 No auditing 4-7 Reserved for IBM's use
GROUPNM	015	00	00	00000008	FF	Char	The current connect group of the user who created this data set.
DSTYPE	016	20	00	00000001	00	Bin	Identifies the data set as a VSAM, non-VSAM (or generic), MODEL or TAPE data set.
							Bit Meaning When Set 0 VSAM data set (non-VSAM if this bit is set to 0) 1 MODEL profile 2 Type = TAPE when set on 3-7 Reserved for IBM's use
LEVEL	017	00	00	00000001	FF	Int	Data set level.
DEVTYPE	018	00	00	00000004	FF	Bin	The type of device on which the data set resides; only for non-model, discrete data sets. For more information, refer to UCBTYP in <i>z/OS MVS Data Areas, Vol 5 (SSAG-XTLST)</i> .
DEVTYPEX	019	00	00	00000008	FF	Char	The EBCDIC name of the device type on which the data set resides; only for non-model, discrete data sets.

Data Set Template

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
GAUDIT	020	20	00	00000001	00	Bin	Global audit flags. (Audit options specified by a user with the AUDITOR or group-AUDITOR attribute.) Bit Meaning When Set 0 Audit all accesses 1 Audit successful accesses 2 Audit accesses that fail 3 No auditing 4-7 Reserved for IBM's use
INSTDATA	021	00	00	00000000	00	Char	Installation data; maximum length=255.
GAUDITQF	025	00	00	00000001	FF	Bin	Global audit FAILURES qualifier. The AUDITQS, AUDITQF, GAUDITQS, and GAUDITQF fields have the following format: Value Meaning When Set X'00' Log access at READ level X'01' Log access at UPDATE level X'02' Log access at CONTROL level X'03' Log access at ALTER level
AUDITQS	022	00	00	00000001	FF	Bin	Audit SUCCESS qualifier.
AUDITQF	023	00	00	00000001	FF	Bin	Audit FAILURES qualifier.
GAUDITQS	024	00	00	00000001	FF	Bin	Global audit SUCCESS qualifier.
WARNING	026	20	00	00000001	00	Bin	Identifies the data set as having (bit 7 is on) or not having the WARNING attribute.
SECLEVEL	027	00	00	00000001	FF	Int	Data set security level.
NUMCTGY	028	10	00	00000004	00	Int	The number of categories.
CATEGORY	029	80	00	00000002	00	Bin	A list of numbers corresponding to the categories to which this data set belongs.
NOTIFY	030	00	00	00000000	00	Char	User to be notified when access violations occur against a data set protected by this profile.
RETPD	031	00	00	00000000	00	Int	The number of days protection is provided for the data set. If used, the field will be a two-byte binary number.
ACL2CNT	032	10	00	00000004	00	Int	The number of program and user combinations currently authorized to access the data set.
PROGRAM	033	80	00	00000008	00	Char	The name of a program currently authorized to access the data set, or a 1-byte flag followed by 7 bytes reserved.
USER2ACS	034	80	00	00000008	00	Char	User ID or group.
PROGACS	035	80	00	00000001	00	Bin	The access authority of the program and user combinations.
PACSCNT	036	80	00	00000002	00	Int	Access count.
ACL2VAR	037	80	00	00000000	00	Char	Additional conditional data, 9-byte length, in which the the 1st byte tells what kind of access is allowed and the remaining 8 bytes contain the data.
FLDCNT	038	10	00	00000004	00		Reserved for IBM's use.
FLDNAME	039	80	00	00000008	00		Reserved for IBM's use.
FLDVALUE	040	80	00	00000000	00		Reserved for IBM's use.
FLDFLAG	041	A0	00	00000001	00		Reserved for IBM's use.
VOLCNT	042	10	00	00000004	00	Int	The number of volumes containing the data set.
VOLSER	043	80	00	00000006	00	Char	A list of the serial numbers of the volumes containing the data set.
ACL2CNT	044	10	00	00000004	00	Int	The number of users and groups currently authorized to access the data set.

Data Set Template

Template Field Name (Character Data)

Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type
045	80	00	00000008	00	Char
046	A0	00	00000001	00	Bin
047	80	00	00000002	00	Int
048	10	00	00000004	00	Int
049	80	00	00000008	00	
050	80	00	00000000	00	
051	A0	00	00000001	00	
052	00	00	00000008	00	Char

Field Being Described

The user ID or group name of each user or group authorized to access the data set.
The access authority that each user or group has for the data set.

Bit Meaning When Set

0	ALTER access
1	CONTROL access
2	UPDATE access
3	READ access
4	EXECUTE access
5-6	Reserved for IBM's use
7	NONE access

The number of times the data set was accessed by each user or group.
Reserved for installation's use.
Reserved for installation's use.
Reserved for installation's use.

Security label.

Field Name Field ID Flag 1 Flag 2 Combination Field IDs Type

Following are the COMBINATION fields of the Data Set Template

DEFDATE	000	40	00	004	000	000	000	000	Char
AUTHDATE	000	40	00	004	000	000	000	000	Char
OWNER	000	40	00	005	000	000	000	000	Char
UACC	000	40	00	012	000	000	000	000	
ACL2	000	40	00	033	034	035	036	037	
ACL2A3	000	40	00	033	034	035	036	000	
ACL2A2	000	40	00	033	034	035	036	000	
ACL2A1	000	40	00	033	034	035	000	000	
FIELD	000	40	00	039	040	041	000	000	
VOLUME	000	40	00	043	000	000	000	000	
ACL	000	40	00	045	046	047	000	000	
ACL1	000	40	00	045	046	000	000	000	
USERDATA	000	40	00	049	050	051	000	000	

Combination.
Fields.

Template

Field Name (Character Data)

Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type
001	00	00	00000000	00	
002	00	00	00000008	FF	Char

Following is the DFP segment of the Data Set Template

DFP	001	00	00	00000000	00	
RESOWNER	002	00	00	00000008	FF	Char

Field Being Described

Start of segment fields

Resource owner; must represent a user ID or group name

Template

Field Name (Character Data)

Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type
001	00	00	00000000	00	
002	10	00	00000004	00	Int
003	80	00	00000000	00	Char

Following is the TME segment of the Data Set Template

TME	001	00	00	00000000	00	
ROLEN	002	10	00	00000004	00	Int
ROLES	003	80	00	00000000	00	Char

Field Being Described

Start of segment fields

Count of role-access specifications

Role-access specifications

General template for the RACF database

The general template describes the fields of general resource profiles in a RACF database.

NOT programming interface information

ACL2RSVD	ENCTYPE	GAUDITQF	PREVKEYV
AUDITQF	FIELD	GAUDITQS	RACLDSP
AUDITQS	FLDCNT	MEMCNT	RACLHDR
CATEGORY	FLDFLAG	MEMLIST	SALT
CURKEY	FLDNAME	NUMCTGY	SSKEY
CURKEYV	FLDVALUE	PREVKEY	

End of NOT programming interface information

Notes:

1. Application developers should not depend on being able to use RACROUTE REQUEST=EXTRACT for the BASE segment fields on any security product other than RACF. These products are expected to support only such segments as DFP and TSO.
2. The TME segment fields are intended to be updated by Tivoli applications, which manage updates, permissions, and cross references among the fields. The TME fields should only be directly updated on an exception basis. See *z/OS Security Server RACF Command Language Reference* for formats of the field data as enforced by the RACF commands. Use caution when directly updating TME fields, as the updates may be overridden by subsequent actions of Tivoli applications.

The contents of the general template are as follows:

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
The following is the BASE segment of the GENERAL template.							
GENERAL	001	00	00	00000000	00		
ENCTYPE	002	00	00	00000001	05	Int	The number (5) corresponding to profiles for resources defined in the class descriptor table.
VERSION	003	00	00	00000001	01	Int	The version field from the profile. Always X'01'.
CLASTYPE	004	00	00	00000001	FF	Int	The class to which the resource belongs (from the ID=class-number operand of the ICHERCDE macro).
DEFDATE	005	00	20	00000003	FF	Date	The date the resource was defined to RACF.
OWNER	006	00	00	00000008	FF	Char	The owner of the resource.
LREFDAT	007	01	20	00000003	FF	Date	The date the resource was last referenced.
LCHGDAT	008	01	20	00000003	FF	Date	The date the resource was last updated.
ACSALTR	009	01	00	00000002	FF	Int	The number of times the resource was accessed with ALTER authority.
ACSCNTL	010	01	00	00000002	FF	Int	The number of times the resource was accessed with CONTROL authority.
ACSUPDT	011	01	00	00000002	FF	Int	The number of times the resource was accessed with UPDATE authority.
ACSREAD	012	01	00	00000002	FF	Int	The number of times the resource was accessed with READ authority.

General Template

Template

Field Name (Character Data)

Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type
UACC	013	20	80	00000001	00	Bin
AUDIT	014	20	00	00000001	00	Bin
LEVEL	015	20	00	00000001	00	Int
GAUDIT	016	20	00	00000001	00	Bin
INSTDATA	017	00	00	00000000	00	Char
GAUDITQF	021	00	00	00000001	FF	Bin
AUDITQS	018	00	00	00000001	FF	Bin
AUDITQF	019	00	00	00000001	FF	Bin

Field Being Described

The universal access authority for the resource.

Bit Meaning When Set

0 ALTER access
1 CONTROL access
2 UPDATE access
3 READ access
4 EXECUTE access
5-6 Reserved for IBM's use
7 NONE access.

Audit flags.

Bit Meaning When Set

0 Audit all accesses
1 Audit successful accesses
2 Audit accesses that fail
3 No auditing
4-7 Reserved for IBM's use

Resource level.

Global audit flags.

Bit Meaning When Set

0 Audit all accesses
1 Audit successful accesses
2 Audit accesses that fail
3 No auditing
4-7 Reserved for IBM's use

Installation data; maximum length=255.

Global audit FAILURES qualifier.

The AUDITQS, AUDITQF, GAUDITQS, and GAUDITQF fields have the following format:

Value Meaning

X'00' Log access at READ authority
X'01' Log access at UPDATE authority
X'02' Log access at CONTROL authority
X'03' Log access at ALTER authority

Audit SUCCESS qualifier. (Audit options specified by a user with the AUDITOR or group-AUDITOR attribute.)

Bit Meaning When Set

0 Audit all accesses
1 Audit successful accesses
2 Audit accesses that fail
3 No auditing
4-7 Reserved for IBM's use

Audit FAILURES qualifier. (Audit options specified by a user with the AUDITOR or group-AUDITOR attribute.)

Bit Meaning When Set

0 Audit all accesses
1 Audit successful accesses
2 Audit accesses that fail
3 No auditing
4-7 Reserved for IBM's use

General Template

Template							Field Being Described
Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	
GAUDITQS	020	00	00	00000001	FF	Bin	Global audit SUCCESS qualifier. (Audit options specified by a user with the AUDITOR or group-AUDITOR attribute.)
							Bit Meaning When Set 0 Audit all accesses 1 Audit successful accesses 2 Audit accesses that fail 3 No auditing 4-7 Reserved for IBM's use
WARNING	022	20	00	00000001	00	Bin	Identifies the data set as having (bit 7 is on) or not having the WARNING attribute.
RESFLG	023	20	00	00000001	00	Bin	Resource profile flags:
							Bit Meaning When Set 0 TAPEVOL may only contain one data set. 1 TAPEVOL profile is automatic. 2 Maintain TVTOC for TAPEVOL. 3-7 Reserved for IBM's use
TVTOCCNT	024	10	00	00000004	00	Int	The number of TVTOC entries.
TVTOCSEQ	025	80	00	00000002	00	Int	The file sequence number of tape data set.
TVTOCCRD	026	80	20	00000003	00	Date	The date the data set was created.
TVTOCIND	027	A0	00	00000001	00	Bin	Data set profiles flag (RACF indicator bit):
							Bit Meaning When Set 1 Discrete data set profile exists 2-7 Reserved for IBM's use
TVTOCDSN	028	80	00	00000000	00	Char	The RACF internal name.
TVTOCVOL	029	80	00	00000000	00	Char	This field is a list of the volumes on which the tape data set resides.
TVTOCRDS	030	80	00	00000000	00	Char	The name used when creating the tape data set; maximum length=255.
NOTIFY	031	00	00	00000000	00	Char	The user to be notified when access violations occur against resource protected by this profile.
LOGDAYS	032	20	00	00000001	00	Bin	The days of the week the TERMINAL may not be used. (Bit 0 equals Sunday, bit 1 equals Monday, and so on).
LOGTIME	033	00	00	00000000	00	Time	The time of the day the TERMINAL may be used.
LOGZONE	034	00	00	00000000	00	Bin	The time zone in which the terminal is located.
NUMCTGY	035	10	00	00000004	00	Int	Number of categories.
CATEGORY	036	80	00	00000002	00	Int	List of categories.
SECLEVEL	037	00	00	00000001	FF	Int	Resource security level.
FLDCNT	038	10	00	00000004	00	Int	Reserved for IBM's use.
FLDNAME	039	80	00	00000008	00		Reserved for IBM's use.
FLDVALUE	040	80	00	00000000	00		Reserved for IBM's use.
FLDFLAG	041	A0	00	00000001	00		Reserved for IBM's use.
APPLDATA	042	00	00	00000000	00	Char	Application data.
MEMCNT	043	10	80	00000004	00	Int	The number of members.
MEMLST	044	80	80	00000000	00	Bin	The resource group member.
VOLCNT	045	10	00	00000004	00	Int	Number of volumes in tape volume set.
VOLSER	046	80	00	00000006	00	Char	Volume serials of volumes in tape volume set.
ACLNT	047	10	80	00000004	00	Int	The number of users and groups currently authorized to access the resource.
USERID	048	80	80	00000008	00	Char	The user ID or group name of each user or group authorized to access the resource.

General Template

Template							Field Being Described
Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	
USERACS	049	A0	80	00000001	00	Bin	The access authority that each user or group has for the resource. Bit Meaning When Set 0 ALTER access 1 CONTROL access 2 UPDATE access 3 READ access 4 EXECUTE access 5-6 Reserved for IBM's use 7 NONE access Note: Each of the above access authority fields have mutually-exclusive bits with the exception of EXECUTE+NONE.
ACSCNT	050	80	00	00000002	00	Int	The number of times the resource was accessed by each user or group.
USRCNT	051	10	00	00000004	00	Int	Reserved for installation's use.
USRNM	052	80	00	00000008	00		Reserved for installation's use.
USRDATA	053	80	00	00000000	00		Reserved for installation's use.
USRFLG	054	A0	00	00000001	00		Reserved for installation's use.
SECLABEL	055	00	00	00000008	00	Char	Security Label (SECLABEL).
ACL2CNT	056	10	00	00000004	00	Int	Number of entries in conditional access list.
ACL2NAME	057	80	00	00000008	00	Bin	1 indicator byte; 7 bytes reserved.
ACL2UID	058	80	00	00000008	00	Char	User ID or group.
ACL2ACC	059	80	00	00000001	00	Bin	Access authority.
ACL2ACNT	060	80	00	00000002	00	Int	Access count.
ACL2RSVD	061	80	00	00000000	00	Bin	Conditional data. Reserved for IBM's use.
RACLHDR	062	00	00	00000020	00	Bin	RACGLIST header.
RACLDSP	063	00	00	00000000	00	Bin	RACGLIST dataspace information.
FILTERCT	064	10	00	00000004	00		Number of names that Hash to this DIGTNMAP Profile.
FLTRLABL	065	80	00	00000000	00		Label associated with this DIGTNMAP Mapping (matches NMAPLABL for user named by FLTRUSER or user irrmulti.)
FLTRSTAT	066	A0	00	00000001	00		Trust status - bit 0 on for trusted.
FLTRUSER	067	80	00	00000000	00		User ID or criteria profile name.
FLTRNAME	068	80	00	00000000	00		Unhashed issuer's name filter used to create this profile name, (max of 255), followed by a separator, (X'4A'), and the unhashed subject's name filter used to create this profile name, (max of 255).
FLTRSVD1	069	80	00	00000000	00		Reserved.
FLTRSVD2	070	80	00	00000000	00		Reserved.
FLTRSVD3	071	80	00	00000000	00		Reserved.
FLTRSVD4	072	80	00	00000000	00		Reserved.
FLTRSVD5	073	80	00	00000000	00		Reserved.
RACDHDR	074	00	08	00000000	00	Bin	CACHECLS header.

Field Name Field ID Flag 1 Flag 2 Combination Field IDs Type

Following is the COMBINATION segment of the GENERAL template.

CREADATE	000	40	00	005 000 000 000 000		Combination.
AUTHDATE	000	40	00	005 000 000 000 000		Fields.
AUTHOR	000	40	00	006 000 000 000 000		
TVTOC	000	48	00	025 026 027 028 029		
	000	40	00	030 000 000 000 000		
LOGINFO	000	40	00	032 033 034 000 000		

General Template

Field Name	Field ID	Flag 1	Flag 2	Combination Field IDs				Type	
FIELD	000	40	00	039	040	041	000	000	
ACL	000	40	00	048	049	050	000	000	
ACL1	000	40	00	048	049	000	000	000	
USERDATA	000	40	00	052	053	054	000	000	
ACL2	000	40	00	057	058	059	060	061	Conditional access list
ACL2A3	000	40	00	057	058	059	060	000	Conditional access list
FLTRLST1	000	40	00	065	066	067	068	000	Combo field for FILTER
FLTRLST2	000	40	00	065	067	068	000	000	Combo field for FILTER
CERTRNG	000	40	00	010	011	009	000	000	Digital Certificate Data.
CERTRNG2	000	40	00	009	011	000	000	000	
CERTRNG3	000	40	00	009	012	013	000	000	

Template

Field Name (Character Data)

Following is the **SESSION** segment of the **GENERAL** template.

Field Name	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type
SESSION	001	00	00	00000000	00	
SESSKEY	002	00	00	00000000	00	Bin
SLSFLAGS	003	20	00	00000001	00	Bin
KEYDATE	004	00	00	00000004	00	Date
KEYINTVL	005	00	00	00000002	00	Int
SLSFAIL	006	00	00	00000002	00	Int
MAXFAIL	007	00	00	00000002	00	Int
SENTCNT	008	10	00	00000004	00	Int
SENTITY	009	80	00	00000035	00	Char
SENTFLCT	010	80	00	00000002	00	Int
CONVSEC	011	20	00	00000001	00	Bin

Field Being Described

Start of segment fields
Session key; maximum length = 8
Session flag byte

Bit **Meaning When Set**
0 SLSLOCK—This profile is locked out

1-7 Reserved for IBM's use
Last date session key was changed. It is in the format *0cyyddF* where *c=0* for 1900-1999 and *c=1* for 2000-2099. For more information on this MVS-returned format, see *z/OS MVS Programming: Assembler Services Guide*.

Number of days before session key expires
Current number of invalid attempts
Number of invalid attempts before lockout
Number of session entities in list
Entity name
Number of failed attempts for this entity
Conversation security.

Value **Meaning**
X'40' Conversation security
X'50' Persistent verification
X'60' User ID and password already verified
X'70' User ID and password already verified plus persistent verification
X'80' Security none

Following is the **DLFDATA** segment of the **GENERAL** template.

DLFDATA	001	00	00	00000000	00	
RETAIN	002	20	00	00000001	00	Bin
JOBNCNT	003	10	00	00000004	00	Int
JOBNAMES	004	80	00	00000000	00	Char

Start of segment fields
Retain flag byte
Count of jobnames
Jobnames; maximum length=8

Following is the **SSIGNON** segment of the **GENERAL** template.

SSIGNON	001	00	00	00000000	00	
SSKEY	002	00	00	00000000	00	Bin

Start of segment fields
Secured signon key

Following is the **STDATA** segment of the **GENERAL** template.

STDATA	001	00	00	00000000	00	
STUSER	002	00	00	00000008	40	Char
STGROUP	003	00	00	00000008	40	Char
FLAGTRUS	004	20	00	00000001	00	Bin

Start of segment fields
User ID or =MEMBER
Group name or =MEMBER
Trusted flag, X'80' = trusted

General Template

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
FLAGPRIV	005	20	00	00000001	00	Bin	Privileged flag, X'80' = privileged
FLAGTRAC	006	20	00	00000001	00	Bin	Trace usage flag X'80' = issue IRR8I2I
Following is the SVFMR segment of the GENERAL template.							
SVFMR	001	00	00	00000000	00		Start of segment fields
SCRIPTN	002	00	00	00000008	00	Char	Script name
PARMN	003	00	00	00000008	00	Char	Parameter name
Following is the CERTDATA segment of the GENERAL template.							
CERTDATA	001	00	00	00000000	00		Start of segment fields
CERT	002	00	00	00000000	00	Bin	Digital Certificate
CERTPRVK	003	00	00	00000000	00	Bin	Private key or key label
RINGCT	004	10	00	00000004	00	Int	Number of key rings associated with this certificate
RINGNAME	005	80	00	00000000	00	Char	Profile name of a ring with which this certificate is associated
CERTSTRT	006	00	00	00000000	00		Date and time from which the certificate is valid. This is an 8-byte TOD format field.
CERTEND	007	00	00	00000000	00		Date and time after which the certificate is not valid. This is an 8-byte TOD format field.
							The CERTCT repeat group identifies the certificates that are associated with a key ring. It is used only with DIGTRING profiles.
CERTCT	008	10	00	00000004	00	Int	The number of certificates associated with this key ring
CERTNAME	009	80	00	00000000	00	Char	The profile name of the certificate
CERTUSAG	010	80	00	00000004	00	Bin	Certificate usage in ring: <ul style="list-style-type: none"> • X'00000000' - PERSONAL • X'00000001' - SITE • X'00000002' - CERTAUTH
CERTDFLT	011	80	00	00000001	00	Bin	Verifies if it is the default certificate: <ul style="list-style-type: none"> • X'00' - Not the default • X'80' - The default
CERTSJDN	012	80	00	00000000	00	Bin	The subject name of the entity to whom the certificate is issued. This field is a BER-encoded format of the subject's distinguished name as contained in the certificate
CERTLABL	013	80	00	00000000	00	Char	Label associated with the certificate
CERTRSV1	014	80	00	00000000	00		Reserved for IBM's use.
CERTRSV2	015	80	00	00000000	00		Reserved for IBM's use.
CERTRSV3	016	80	00	00000000	00		Reserved for IBM's use.
CERTRSV4	017	80	00	00000000	00		Reserved for IBM's use.
CERTRSV5	018	80	00	00000000	00		Reserved for IBM's use.
CERTRSV6	019	80	00	00000000	00		Reserved for IBM's use.
CERTRSV7	020	80	00	00000000	00		Reserved for IBM's use.
CERTRSV8	021	80	00	00000000	00		Reserved for IBM's use.
CERTRSV9	022	80	00	00000000	00		Reserved for IBM's use.
CERTRSVA	023	80	00	00000000	00		Reserved for IBM's use.
CERTRSVB	024	80	00	00000000	00		Reserved for IBM's use.
CERTRSVC	025	80	00	00000000	00		Reserved for IBM's use.
CERTRSVD	026	80	00	00000000	00		Reserved for IBM's use.
CERTRSVE	027	80	00	00000000	00		Reserved for IBM's use.
CERTRSVF	028	80	00	00000000	00		Reserved for IBM's use.
CERTRSVG	029	80	00	00000000	00		Reserved for IBM's use.
CERTRSVH	030	80	00	00000000	00		Reserved for IBM's use.

General Template

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
CERTRSVI	031	80	00	00000000	00		Reserved for IBM's use.
CERTRSVJ	032	80	00	00000000	00		Reserved for IBM's use.
CERTRSVK	033	80	00	00000000	00		Reserved for IBM's use.
CERTPRVT	034	00	00	00000004	00	Bin	Private key type: <ul style="list-style-type: none"> • X'00000000' - No private key • X'00000001' - PKCS DER-encoded • X'00000002' - ICSF token label • X'00000003' - PCICC label
CERTPRVS	035	00	00	00000004	00	Int	Private key size in bits
CERTLSER	036	00	00	00000008	00	Bin	The low order 8 bytes of the last certificate that was signed with this key. This field is used with DIGTCERT profiles only
RINGSEQN	037	00	00	00000004	00	Int	Ring change count
Following is the TME segment of the GENERAL template.							
TME	001	00	00	00000000	00		Start of segment fields
PARENT	002	00	00	00000000	00	Char	Parent name
CHILDN	003	10	00	00000004	00	Int	Count of children
CHILDREN	004	80	00	00000000	00	Char	Child names
RESN	005	10	00	00000004	00	Int	Count of resource-access specifications
RESOURCE	006	80	00	00000000	00		Resource-access specifications
GROUPN	007	10	00	00000004	00	Int	Count of groups
GROUPS	008	80	00	00000008	00		Group names
ROLEN	009	10	00	00000004	00	Int	Count of role-access specifications
ROLES	010	80	00	00000000	00	Char	Role-access specifications
Following is the KERB segment of the GENERAL template							
KERB	001	00	00	00000000	00		Start of segment fields
KERBNAME	002	00	00	00000000	00	Char	Kerberos realm name
MINTKTLF	003	00	00	00000000	00	Char	Minimum ticket life
MAXTKTLF	004	00	00	00000000	00	Char	Maximum ticket life
DEFTKTLF	005	00	00	00000000	00	Char	Default ticket life
SALT	006	00	00	00000000	00	Char	Current key salt
ENCTYPE	007	00	00	00000000	00	Char	Encryption type
CURKEYV	008	00	00	00000000	00	Char	Current key version
CURKEY	009	00	00	00000000	00	Char	Current DES key
PREVKEYV	010	00	00	00000000	00	Char	Previous key version
PREVKEY	011	00	00	00000000	00	Char	Previous DES key
ENCRYPT	012	00	00	00000004	55	Char	Encryption types for SETROPTS KERBLVL(1)
Following is the PROXY segment of the GENERAL template							
PROXY	001	00	00	00000000	00		Start of segment fields
LDAPHOST	002	00	00	00000000	00	Char	LDAP server URL; maximum length: 1023
BINDDN	003	00	00	00000000	00	Char	Bind distinguished name; maximum length: 1023
BINDPW	004	00	08	00000000	00	Char	Bind password; maximum length: 128
BINDPWKY	005	00	08	00000071	00	Char	Bind password mask or encrypt key
Following is the EIM segment of the GENERAL template							
DOMAINDN	1	00	00	00000000	00	Char	EIM Domain Distinguished Name
OPTIONS	2	00	00	00000004	55	Char	EIM Options
LOCALREG	3	00	00	00000000	00	Char	Local Registry Name

Reserved templates for the RACF database

Five unused templates are defined for future use. The installation must leave this space reserved and not use it.

Reserved Templates

The contents of the reserved templates are:

Template Field Name (Character Data)	Field ID	Flag 1	Flag 2	Field Length Decimal	Default Value	Type	Field Being Described
RSVTMP0x	001	00	00	00000000	00		'x' can range from 2 to 6.
ENTYPE	002	00	00	00000001	00		The number corresponding to the type of profile being described.
VERSION	003	00	00	00000001	00		Template version number.

Appendix E. Event Code Qualifier Descriptions

Event Codes and Event Code Qualifiers

The RACF event code (found in the SMF80EVT field of the SMF record) and the RACF event code qualifier (found in the SMF80EVQ field of the SMF record) are determined during RACF processing. This section explains the meaning of each qualifier code by event.

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

This event is logged by RACROUTE REQUEST=VERIFY and RACROUTE REQUEST=VERIFYX. Installation exit ICHRIX02 can change the return code of the RACROUTE REQUEST=VERIFY or RACROUTE REQUEST=VERIFYX request to any value. The return code significantly influences the corresponding audit record's event code 1 qualifier. You should be familiar with any ICHRIX02 processing in effect for your installation. See *z/OS Security Server RACF System Programmer's Guide* for details.

For this event, code qualifiers 0 and 8 do not exist as type 80 records. They are contained in the unloaded records from the RACF SMF data unload utility (IRRADU00) and as reports and reformatted records from the RACF report writer (RACFRW).

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

- 0(0) SUCCESSFUL INITIATION** The job began successfully.
- 1(1) INVALID PASSWORD** The password specified on the job card or at logon is incorrect.
- 2(2) INVALID GROUP** The user tried to log on or to initiate a job using a group that the user is not a member of.
- 3(3) INVALID OIDCARD** Operator identification cards are used at the installation, and the data received from the one used does not match that of the user's profile.
- 4(4) INVALID TERMINAL/CONSOLE** The user is not authorized to the port of entry (POE). There are four kinds of POEs, each with its own profile class: APPCPORT, CONSOLE, JESINPUT, and TERMINAL. One of the following occurred:
 - The port of entry is active but the user is not authorized.
 - The user is denied access because of conditional days/times in the user profile.
 - The user is denied access because of conditional days/times in the class profile (TERMINAL class only).
- 5(5) INVALID APPLICATION** The APPL class is active, and the user is trying to log on to an application without authorization.
- 6(6) REVOKED USER ID ATTEMPTING ACCESS** The user ID specified on the logon or job card has been revoked. One of the following occurred:
 - The installation-defined limit of password attempts was reached at an earlier time.
 - The inactive interval was reached.
 - The revoke date in the user's profile is in effect.

- The RACF administrator revoked the user ID.

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

- 7(7) USER ID AUTOMATICALLY REVOKED** The user ID has been automatically revoked. One of the following occurred:
- The installation-defined limit of password attempts was reached.
 - The user has been inactive longer than the system inactive interval set by the SETROPTS command.
- 8(8) SUCCESSFUL TERMINATION** The job completed successfully.
- 9(9) UNDEFINED USER ID** The user ID specified on the job card or at logon is not defined to the RACF database.
- 10(A) INSUFFICIENT SECURITY LABEL AUTHORITY** One of the following occurred:
- SETROPTS MLS FAILURES is in effect and the user's security label does not dominate the submitter's security label. Two exceptions are explained under Qualifier 20.
 - SETROPTS MLACTIVE FAILURES is in effect and the job card/logon attempt does not specify a valid security label. One exception is explained under Qualifier 21.
- 11(B) NOT AUTHORIZED TO SECURITY LABEL** The user is not authorized to the security label specified. One exception is explained under Qualifier 22.
- 12(C) SUCCESSFUL RACINIT INITIATION** The job or user was verified.
- 13(D) SUCCESSFUL RACINIT DELETE** The job completed or the user logged off.
- 14(E) SYSTEM NOW REQUIRES MORE AUTHORITY** SETROPTS MLQUIET is in effect. If this is a user verification, the user is not a console operator and does not have the SPECIAL attribute. If this is a job verification, the job is not part of the trusted computing base (TCB). The verification fails.
- 15(F) REMOTE JOB ENTRY—JOB NOT AUTHORIZED** The submitting node is not authorized to the system; a NODES profile prevents remote job entry. The profile has the format 'submit_node.RUSER.userid' and has a UACC of NONE.

Surrogate Function Qualifiers:

Qualifiers 16, 17, and 18 involve the use of the surrogate function, and occur if any of the following conditions is met:

- The SURROGAT class is active.
- General resource profiles of the SURROGAT class are defined for the job card's user ID, and the user ID submitting the job is permitted to the profile with at least READ access.
- The submitter is authorized to the security label of the job.

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

- 16(10) SURROGATE CLASS IS INACTIVE** The SURROGAT class is inactive. The job card has a user ID that is different from the submitter's user ID, and there is no password specified.

- 17(11) SUBMITTER IS NOT AUTHORIZED BY USER** The SURROGAT class is active. Either there is no SURROGAT profile for the job card's user ID, or the submitter's user ID is not permitted to the profile.
- 18(12) SUBMITTER IS NOT AUTHORIZED TO SECURITY LABEL** The SECLABEL class is active and there is a security label on the job card. The submitter is not authorized to the security label specified on the job card.
- 19(13) USER IS NOT AUTHORIZED TO JOB** The JESJOBS class is active, and the user is not authorized to the jobname.
- 20(14) WARNING—INSUFFICIENT SECURITY LABEL AUTHORITY** One of the following occurred:
- SETROPTS MLS WARNING is in effect and the security label on the job card does not dominate the submitter's security label.
 - SETROPTS MLS FAILURES is in effect, the user's security label does not dominate the submitter's, and the user has the SPECIAL attribute.
 - SETROPTS MLS FAILURES and SETROPTS COMPATMODE are in effect, the user's security label does not dominate the submitter's, and the submitter's or the job owner's security label is the default.
- The verification does not fail.
- 21(15) WARNING—SECURITY LABEL MISSING FROM JOB, USER, OR PROFILE** One of the following occurred:
- MLACTIVE WARNING is in effect, and the job card or logon attempt did not specify a valid security label.
 - MLACTIVE FAILURES is in effect, the user has the SPECIAL attribute, and a valid security label is not specified.
- The verification does not fail.
- 22(16) WARNING—NOT AUTHORIZED TO SECURITY LABEL** The user has the SPECIAL attribute, the security label is SYSHIGH, and the user does not have authority to it. The verification does not fail.
- 23(17) SECURITY LABELS NOT COMPATIBLE** SETROPTS MLS is not active, the submitter's user ID is different from the user ID on the job card, and the submitter's and the user's security labels are disjoint (neither one dominates the other).
- One exception is listed under Qualifier 24.
- 24(18) WARNING—SECURITY LABELS NOT COMPATIBLE** SETROPTS MLS is not active, the submitter's user ID is different from the user ID on the job card, the submitter's and user's security labels are disjoint, SETROPTS COMPATMODE is in effect, and the submitter's or user's security label is the default. The verification does not fail.
- 25(19) CURRENT PASSWORD HAS EXPIRED** The user's password has expired for one of the following reasons:
- The installation specification in SETROPTS PASSWORD INTERVAL command
 - Creation of the password in the ADDUSER command
 - Alteration of the password with the ALTUSER PASSWORD command
- 26(1A) INVALID NEW PASSWORD** The new password specified may be incorrect because:
- It is all blanks.

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

27(1B)

VERIFICATION FAILED BY INSTALLATION The installation exit ICHRIX01 or ICHRIX02 failed the request.

28(1C)

GROUP ACCESS HAS BEEN REVOKED The user's membership to the group specified has been revoked.

29(1D)

OIDCARD IS REQUIRED An OIDCARD is required by the installation but none was given.

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

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

See *z/OS Security Server RACF Security Administrator's Guide* for details on NJE.

31(1F) WARNING—UNKNOWN USER FROM TRUSTED NODE PROPAGATED

The combination of having a trusted node submit a job with the undefined user ID warrants this logging. The verification does not fail.

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

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

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

Event 2(2): RESOURCE ACCESS

This event is logged by RACROUTE REQUEST=AUTH.

This event is also logged by RACROUTE REQUEST=FASTAUTH, but only for qualifiers 0, 1, 3, 6, and 13.

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

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

- 1(1) INSUFFICIENT AUTHORITY** The user does not have authorization to the resource.
- 2(2) PROFILE NOT FOUND—RACFIND SPECIFIED ON MACRO** If the request is AUTH, the RACFIND keyword equaled YES on the authorization request, specifying that a discrete profile should exist for the resource. No discrete or generic RACF protection was found.
- If the request is FASTAUTH, the program is not controlled and the PADS data sets are open.
- 3(3) ACCESS PERMITTED DUE TO WARNING** The user does not have proper authority to the resource. However, the resource's profile has the WARNING option and allows the access.

Exceptions

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

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

Exceptions

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

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

The exceptions in Qualifier 4 also apply.

- 6(6) INSUFFICIENT CATEGORY/SECLEVEL** The installation uses categories or security levels as separate entities. One of the following occurred:
- The user's SECLEVEL is less than the SECLEVEL of the resource.
 - The user is not a member of every CATEGORY associated with the resource.

- 7(7) INSUFFICIENT SECURITY LABEL AUTHORITY** The SECLABEL class is active and one of the following occurred:
- The user's security label does not dominate the resource's.
 - The user does not have a security label, but the resource does.
 - SETROPTS MLACTIVE FAILURES is in effect, and either the user or the resource is missing a security label. One exception is explained in Qualifier 8.
 - The resource's class requires reverse domination checking, and the resource's security label does not dominate the user's.

- SETROPTS MLS FAILURES is in effect; the user's security label does not equal the resource's, and the requested access is UPDATE or CONTROL. One exception is explained under Qualifier 9.

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

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

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

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

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

See the *z/OS Security Server RACF Command Language Reference* for more information.

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

See the *z/OS Security Server RACF Command Language Reference* for more information.

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

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

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

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

Exceptions

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

14(E) WARNING—NON-MAIN EXECUTION ENVIRONMENT Non-MAIN execution environment was detected while in ENHANCED PGMSECURITY mode. Conditional access for Program Access to Data Sets (PADS) or access to EXECUTE-controlled program is temporarily allowed.

| **15(F) CONDITIONAL ACCESS ALLOWED VIA BASIC MODE PROGRAM**

| Conditional access for Program Access to Data Sets (PADS) or access to
| EXECUTE-controlled program is allowed through the BASIC mode program
| while in ENHANCED PGMSECURITY mode.

Event 3(3): ADDVOL/CHGVOL

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

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

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

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

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

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

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

Exception

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

Event 4(4): RENAME RESOURCE

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

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

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

- The user has sufficient authority to rename the resource.

- The SECLABEL class is active, SETROPTS MACTIVE WARNING is in effect, and the user or the resource does not have a security label.
- 1(1) INVALID GROUP** The resource to be renamed is a data set, and the high-level qualifier of the new data set is not a valid group or user ID.
- 2(2) USER NOT IN GROUP** The resource is a data set, RACFIND is not set to NO, the high-level qualifier of the new data set name is a group, and the user does not belong to that group.
- 3(3) INSUFFICIENT AUTHORITY** One of the following occurred:
- SETROPTS GENERICOWNER is in effect, and renaming the profile would violate GENERICOWNER rules.
 - The resource is a data set, and the high-level qualifier is a group or user ID. The user is not authorized to create a new data set by the generic profile protecting the new name, and the high-level qualifier of the new data set name is beyond the scope of the user.
 - The resource is an SFS file or directory, and the second qualifier is a user ID. The user is not authorized to create a new file or directory by the generic profile protecting the new name, and the second qualifier of the new file or directory name is beyond the scope of the user.

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

- 4(4) RESOURCE NAME ALREADY DEFINED** The requested new name already has a discrete profile defined. The return code of the RENAME is 4.
- 5(5) USER NOT DEFINED TO RACF** The installation's naming convention routine has indicated that the high-level qualifier is a user ID that is not defined to RACF. One of the following occurred:
- RACFIND is not set to NO.
 - The resource is protected by a generic or global profile, and the user does not have ALTER access to it.
- 6(6) RESOURCE NOT PROTECTED** SETROPTS PROTECTALL FAILURES is in effect, and the new data set name is not protected by a profile.
- 7(7) WARNING—RESOURCE NOT PROTECTED** SETROPTS PROTECTALL WARNINGS is in effect, and the new data set name is not protected by a profile.
- The RENAME is allowed.
- 8(8) USER IN SECOND QUALIFIER IS NOT RACF DEFINED** The second qualifier of the new name is not a valid user ID.
- 9(9) LESS SPECIFIC PROFILE EXISTS WITH DIFFERENT SECLABEL** The SECLABEL class is active, SETROPTS MLSTABLE is in effect, and there is a less specific generic profile existing for the new name with a different security label. Renaming this resource would violate SETROPTS MLSTABLE rules.
- 10(A) INSUFFICIENT SECURITY LABEL AUTHORITY** The SECLABEL class is active, SETROPTS MLS FAILURES is in effect, and the user is not authorized to the security label of the resource to be renamed.
- 11(B) RESOURCE NOT PROTECTED BY SECURITY LABEL** The SECLABEL class is active, SETROPTS MLS FAILURES is in effect, and the profile covering the old resource name does not have a security label.
- 12(C) NEW NAME NOT PROTECTED BY SECURITY LABEL** The SECLABEL

class is active, SETROPTS MLS FAILURES is in effect, and the profile that would cover the new resource name does not have a security label.

- 13(D) NEW SECLABEL MUST DOMINATE OLD SECLABEL** The SECLABEL class is active, SETROPTS MLS FAILURES is in effect, and the security label of the profile covering the new resource name does not dominate the security label of the profile covering the old resource name.
- 14(E) INSUFFICIENT SECURITY LABEL AUTHORITY** The SECLABEL class is active, SETROPTS MLS WARNING is in effect, and the user is not authorized to the security label of the profile. The RENAME is allowed.
- 15(F) WARNING—RESOURCE NOT PROTECTED BY SECURITY LABEL** The SECLABEL class is active, SETROPTS MLS WARNING is in effect, and the profile covering the old resource name does not have a security label. The RENAME is allowed.
- 16(10) WARNING—NEW NAME NOT PROTECTED BY SECURITY LABEL** The SECLABEL class is active, SETROPTS MLS WARNING is in effect, and the profile that would cover the new resource name does not have a security label. The RENAME is allowed.
- 17(11) WARNING—NEW SECLABEL MUST DOMINATE OLD SECLABEL** The SECLABEL class is active, SETROPTS MLS WARNING is in effect, and the security label of the profile covering the new resource name does not dominate the security label of the profile covering the old resource name. The RENAME does not fail.

Event 5(5): DELETE RESOURCE

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

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

- 0(0) SUCCESSFUL SCRATCH** The resource profile was deleted.
- 1(1) RESOURCE NOT FOUND** The resource profile was not found.
- 2(2) INVALID VOLUME** The class is DATASET, and the data set does not reside on the volume specified.

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

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

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

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

Event 7(7): DEFINE RESOURCE

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

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

- 0(0) SUCCESSFUL DEFINITION**
- The user had sufficient authority to define the resource.
 - The SECLABEL class is active, SETROPTS MACTIVE WARNING is in effect, and the user or the resource does not have a security label.

- 1(1) GROUP UNDEFINED** The resource to be defined is a data set, and the high-level qualifier is not a valid group or user ID.
- 2(2) USER NOT IN GROUP** The resource is a data set, RACFIND is not set to NO, the high-level qualifier is a group, and the user does not belong to that group.
- 3(3) INSUFFICIENT AUTHORITY** One of the following occurred:
- SETROPTS GENERICOWNER is in effect and defining the profile would violate GENERICOWNER rules.
 - For general resources, the user is not authorized to define profiles in the class.
 - The resource is a data set, and the high-level qualifier of the resource is a group or user ID. The user is not authorized to create a new data set by the generic profile protecting the new name, and the high-level qualifier of the new data set name is beyond the scope of the user.
 - The resource is an SFS file or directory, and the second qualifier is a user ID. The user is not authorized to create a new file or directory by the generic profile protecting the new name, and the second qualifier of the new file or directory name is beyond the scope of the user.

See z/OS Security Server RACF Security Administrator's Guide.

- 4(4) RESOURCE NAME ALREADY DEFINED** The requested name already has a discrete profile defined. The return code of the DEFINE is 4.
- 5(5) USER NOT DEFINED TO RACF** The installation's naming convention routine has indicated that the high-level qualifier is a user ID that is not defined to RACF. One of the following occurred:
- RACFIND is not set to NO.
 - The resource is protected by a generic or global profile, and the user does not have ALTER access to it.
- 6(6) RESOURCE NOT PROTECTED** SETROPTS PROTECTALL FAILURES is in effect, and the data set to be defined will not be protected by a profile.
- 7(7) WARNING—RESOURCE NOT PROTECTED** SETROPTS PROTECTALL WARNINGS is in effect, and the data set to be defined will not be protected by a profile. The DEFINE is allowed.
- 8(8) WARNING—SECURITY LABEL MISSING FROM JOB, USER, OR PROFILE** The SECLABEL and TAPEVOL classes are active. SETROPTS MACTIVE WARNING is in effect, and the TAPEVOL profile is without a security label. The DEFINE is allowed.
- 9(9) INSUFFICIENT SECURITY LABEL AUTHORITY** The SECLABEL and TAPEVOL classes are active. SETROPTS MLS WARNING is in effect, and the user's security label does not dominate the one found in the TAPEVOL profile.
- The DEFINE is allowed.
- 10(A) USER IN SECOND QUALIFIER IS NOT RACF-DEFINED** The second qualifier of the name is not a valid user ID.
- 11(B) INSUFFICIENT SECURITY LABEL AUTHORITY** The SECLABEL class is active, and one of the following occurred:
- SETROPTS MACTIVE FAILURES is in effect, and the user is missing a security label.

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

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

Defining this resource would violate SETROPTS MLSTABLE rules.

Event 8(8)–25(19): COMMANDS

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

- 0(0) NO VIOLATIONS DETECTED** The RACF command was issued successfully. This qualifier applies to all RACF commands.
- 1(1) INSUFFICIENT AUTHORITY** The user did not have the authority to issue the RACF command. This qualifier applies to all RACF commands.
- 2(2) KEYWORD VIOLATIONS DETECTED** The user had the authority to issue the RACF command, but not to all the keywords that were specified. Keywords that the user is not authorized to use are ignored. For example, a user with the SPECIAL attribute but without the AUDITOR attribute can issue the ALTUSER command, but not with the GLOBALAUDIT keyword. This qualifier applies to all RACF commands.
- 3(3) SUCCESSFUL LISTING OF DATASETS** This logs the successful use of LISTDSD DSNS.
- 4(4) SYSTEM ERROR IN LISTING OF DATA SETS** This logs an error in attempting LISTDSD DSNS.

Notes:

1. When the SETROPTS command is issued with a keyword that contains an asterisk (*), the asterisk is displayed in the output. For example, if you issue the command SETROPTS AUDIT(*), the output contains AUDIT(*)
2. When the SETROPTS command is issued with a keyword that lists more than ten classes, the output lists the first ten classes and displays the remaining number as an ellipsis. For example, if you issue the command SETROPTS CLASSACT(class1 class2 class3 class4 class5 class6 class7 class8 class9 class10 class11 class12), the output appears as CLASSACT(class1 class2 class3 class4 class5 class6 class7 class8 class9 class10 ...(00002)).
3. When the RVARY command is issued, the DATASET keyword lists the names of as many RACF databases as can fit in the 1024 character output. The remainder are shown as an ellipsis (...(nnnnn)).
4. When the RVARY command is issued with the NOCLASSACT(*) keyword or with more than ten classes specified, the output lists the first ten classes. The remaining classes are shown as an ellipsis.

Event 26(1A): APPCLU

This event is logged by RACROUTE REQUEST=AUDIT,EVENT='APPCLU'. This event applies to establishing a session between two logical units (referred to as the

local LU and the partner LU) in accordance with the System Network Architecture (SNA). VTAM and CICS call RACF for security information stored in general resource profiles in the APPCLU class.

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

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

- 0(0) PARTNER VERIFICATION WAS SUCCESSFUL** The handshaking was successful. The LUs established a connection.
- 1(1) SESSION ESTABLISHED WITHOUT VERIFICATION** No handshaking was done, but the LUs were still allowed to establish a connection, with the knowledge that the partners were not verified.
- 2(2) LOCAL LU KEY WILL EXPIRE IN 5 DAYS OR LESS** The handshaking was successful; this qualifier was set to tell users when the local LU's session key would expire.
- 3(3) PARTNER LU ACCESS HAS BEEN REVOKED** Too many unsuccessful attempts were made at matching the session key.
- 4(4) PARTNER LU KEY DOES NOT MATCH THIS LU KEY** An attempt was made to establish a session, but the session keys did not match. For example, the two sets of identical data encrypted with the two keys did not match.
- 5(5) SESSION TERMINATED FOR SECURITY REASONS** One or both of the APPCLU profiles involved have the keyword LOCK specified in their session information, preventing any connections from being made. This keyword enables the security administrator to temporarily prevent specific connections without deleting any profiles.
- 6(6) REQUIRED SESSION KEY NOT DEFINED** The local LU had VERIFY=REQUIRED coded on its APPL statement, indicating that session level verification must be used on all sessions with the LU. One of the following occurred:
 - The local LU is the primary LU and no password was defined in RACF for the LU pair.
 - The partner LU is the primary LU, but the bind it sent to the local LU did not contain random data (which would indicate that the partner is using session level verification also).
- 7(7) POSSIBLE SECURITY ATTACK BY PARTNER LU** The local LU sent out a random number to another LU as part of the handshaking process of establishing a session. That same number then came in from a third LU for the local LU to encrypt. It is a coincidence that the same number is chosen; the number is 64 bits of random data.

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

- 9(9) **SESSION KEY NOT DEFINED FOR THIS LU** The local LU had VERIFY=OPTIONAL coded on its APPL statement. No password was defined in the local LU's RACF profile for the LU-LU pair, indicating that session level verification may not be used to establish sessions with this LU. However, the partner LU tried to establish a session using session level verification.
- 10(A) **SNA SECURITY-RELATED PROTOCOL ERROR** The LU trying to establish a connection is not responding correctly according to the handshaking protocol.
- 11(B) **PROFILE CHANGE DURING VERIFICATION** The handshaking was attempted, but it is evident that one of the LU's profiles (specifically the session key) changed in the middle of the handshaking, making its success impossible.
- 12(C) **EXPIRED SESSION KEY** The session key in one or both of the APPCLU profiles has expired.

Event 27(1B): GENERAL AUDITING

This event is logged by RACROUTE REQUEST=AUDIT,EVENT='GENERAL'. RACF does not make any authority checks for this event.

The explanations of the event code qualifiers for Event 27 are:

0 - 99 GENERAL AUDIT RECORD WRITTEN

Qualifiers 0 to 99 can be used for Event 27. These qualifiers are installation defined.

Event 28(1C)–58(3A): z/OS UNIX EVENT TYPES

Events 28 through 58 apply to z/OS UNIX. The following qualifier codes are used for each event:

- 28(1C) **DIRECTORY SEARCH**
 - 0(0) Access allowed
 - 1(1) Not authorized to search directory
- 29(1D) **CHECK ACCESS TO DIRECTORY**
 - 0(0) Access allowed
 - 1(1) Caller does not have requested access authority
- 30(1E) **CHECK ACCESS TO FILE**
 - 0(0) Access allowed
 - 1(1) Caller does not have requested access authority
- 31(1F) **CHAUDIT**
 - 0(0) File's audit options changed
 - 1(1) Caller does not have authority to change user audit options of specified file
 - 2(2) Caller does not have authority to change auditor audit options
- 32(20) **CHDIR**
 - 0(0) Current working directory changed

	* Failures logged as directory search event types
33(21)	CHMOD
	0(0) File's mode changed
	1(1) Caller does not have authority to change mode of specified file
34(22)	CHOWN
	0(0) File's owner or group owner changed
	1(1) Caller does not have authority to change owner or group owner of specified file
35(23)	CLEAR SETID BITS FOR FILE
	0(0) S_ISUID, S_ISGID, and S_ISVTX bits changed to zero (write)
	No failure cases
36(24)	EXEC WITH SETUID/SETGID
	0(0) Successful change of UIDs and GIDs
	No failure cases
37(25)	GETPSENT
	0(0) Access allowed
	1(1) Not authorized to access specified process
38(26)	INITIALIZE z/OS UNIX PROCESS (DUB)
	0(0) z/OS UNIX process successfully initiated
	1(1) User not defined as a z/OS UNIX user (no user profile or no OMVS segment)
	2(2) User incompletely defined as a z/OS UNIX user (no UID in user profile)
	3(3) User's current group has no GID
39(27)	z/OS UNIX PROCESS COMPLETION (UNDUB)
	0(0) Process completed
	No failure cases
40(28)	KILL
	0(0) Access allowed
	1(1) Not authorized to access specified process
41(29)	LINK
	0(0) New link created
	* Failures logged as directory search or check access event types
42(2A)	MKDIR
	0(0) Directory successfully created
	* Failures logged as directory search or check access event types

43(2B)	MKNOD
	0(0) Successful creation of a node
	* Failures logged as directory search or check access event types
44(2C)	MOUNT FILE SYSTEM
	0(0) Successful mount
	* Failures logged as ck_priv event type
45(2D)	OPEN (NEW FILE)
	0(0) File successfully created
	* Failures logged as directory search or check access event types
46(2E)	PTRACE
	0(0) Access allowed
	1(1) Not authorized to access specified process
47(2F)	RENAME
	0(0) Rename successful
	* Failures logged as directory search or check access event types
48(30)	RMDIR
	0(0) Successful rmdir
	* Failures logged as directory search or check access event types
49(31)	SETEGID
	0(0) Successful change of effective GID
	1(1) Not authorized to setegid
50(32)	SETEUID
	0(0) Successful change of effective UID
	1(1) Not authorized to seteuid
51(33)	SETGID
	0(0) Successful change of GIDs
	1(1) Not authorized to setgid
52(34)	SETUID
	0(0) Successful change of UIDs
	1(1) Not authorized to setuid
53(35)	SYMLINK
	0(0) Successful symlink
	* Failures logged as directory search or check access event types
54(36)	UNLINK

	0(0)	Successful unlink
	*	Failures logged as directory search or check access event types
55(37)		UNMOUNT FILE SYSTEM
	0(0)	Successful unmount
	*	Failures logged as ck_priv event type
56(38)		CHECK FILE OWNER
	0(0)	User is the owner
	1(1)	User is not the owner
57(39)		CK_PRIV
	0(0)	User is authorized
	1(1)	User not authorized to use requested function
58(3A)		OPEN SLAVE TTY
	0(0)	Access allowed
	1(1)	Not authorized to access specified process

Event 59(3B): RACLINK EVENT TYPES

The explanations of the event code qualifiers for Event 59 are:

0(0)	No violation detected
1(1)	Insufficient authority
2(2)	Keyword violation detected
3(3)	Association already defined
4(4)	Association already approved
5(5)	Association does not match
6(6)	Association does not exist
7(7)	Invalid password or revoked user ID

Event 60(3C)–62(3E): z/OS UNIX XPG4 EVENT TYPES

60(3C)	CHECK IPC ACCESS
	0(0) Access allowed
	1(1) Caller does not have requested access authority
61(3D)	MAKE ISP
	0(0) Successful creation of ISP
62(3E)	R_IPC CONTROL
	0(0) Access allowed
	1(1) Caller does not have requested access authority

Event 63(3F): z/OS UNIX SETGROUPS EVENT TYPE

0(0)	Successful
-------------	------------

1(1) Not authorized

Event 64(40): X/OPEN SINGLE UNIX SPECIFICATION EVENT TYPES

64(40) CHECK OWNER TWO FILES

0(0) User is the owner

1(1) User is not the owner

Event 65(41): z/OS UNIX PASSING OF ACCESS RIGHTS EVENT TYPES

65(41) R_AUDIT

0(0) Successful r_audit

No failure cases

Event 66(42)–67(43): CERTIFICATE EVENT TYPES

66(42) RACDCERT

0(0) No violation detected

1(1) Insufficient authority

67(43) initACEE

0(0) Successful certificate registration

1(1) Successful certificate deregistration

2(2) Insufficient authority to register a certificate

3(3) Insufficient authority to deregister a certificate

4(4) No user ID found for certificate

5(5) Certificate is not trusted

6(6) Successful CERTAUTH certificate registration

7(7) Insufficient authority to register the CERTAUTH certificate

Event 68(44): GRANT OF INITIAL KERBEROS TICKET

68(44) Kerberos

0(0) Success

1(1) Failure

Event 69(45): R_PKIServ GENCERT

69(45) RPKIGENC

0(0) Successful certificate GENCERT request

1(1) Unsuccessful certificate GENCERT request due to insufficient authority

2(2) Successful REQCERT request

3(3) Insufficient authority for REQCERT

4(4) Successful GENRENEW request

- 5(5) Insufficient authority for GENRENEW
- 6(6) Successful REQRENEW request
- 7(7) Insufficient authority for REQRENEW

Event 70(46): R_PKIServ EXPORT

70(46)

RPKIEXPT

- 0(0) Successful certificate EXPORT request
- 1(1) Unsuccessful certificate EXPORT request due to insufficient authority
- 2(2) Incorrect pass phrase specified for EXPORT

Event 71(47): POLICY DIRECTOR ACCESS CONTROL DECISION

71(47)

PDACCESS

This event is reserved for use by Policy Director Authorization Services.

- 0(0) Authorized
- 1(1) Not authorized but permitted because of warning mode
- 2(2) Not authorized due to insufficient traverse authority but permitted because of warning mode
- 3(3) Not authorized due to time-of-day check but permitted because of warning mode
- 4(4) Not authorized
- 5(5) Not authorized due to insufficient traverse authority
- 6(6) Not authorized due to time-of-day check

Event 72(48): R_PKIServ QUERY

72(48)

RPKIREAD

- 0(0) Successful admin QUERY or DETAILS request
- 1(1) Insufficient authority for admin QUERY or DETAILS
- 2(2) Successful VERIFY request
- 3(3) Insufficient authority for VERIFY
- 4(4) Incorrect VERIFY certificate, no record found for this certificate

Event 73(49): R_PKIServ UPDATEREQ

73(49)

RPKIUPDR

- 0(0) Successful admin UPDATEREQ
- 1(1) Insufficient authority for admin UPDATEREQ

Event 74(4A): R_PKIServ UPDATECERT

74(4A)

RPKIUPDC

- 0(0) Successful admin UPDATECERT request
- 1(1) Insufficient authority for admin UPDATECERT
- 2(2) Successful REVOKE request
- 3(3) Insufficient authority for REVOKE

Event 75(4B): ACCESS CONTROL LISTS SETFACL

75(4B)

SETFACL

- 0(0) ACL entry added, changed, or deleted
- 1(1) Caller does not have authority to change ACL of specified file

Event 76(4C): ACCESS CONTROL LISTS DELFACL

76(4C)

DELFACL

- 0(0) Entire ACL deleted
- 1(1) Caller does not have authority to remove ACL of specified file

Appendix F. Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in z/OS enable users to:

- Use assistive technologies such as screen-readers and screen magnifier software
- Operate specific or equivalent features using only the keyboard
- Customize display attributes such as color, contrast, and font size

Using assistive technologies

Assistive technology products, such as screen-readers, function with the user interfaces found in z/OS. Consult the assistive technology documentation for specific information when using it to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. Refer to *z/OS TSO/E Primer*, *z/OS TSO/E User's Guide*, and *z/OS ISPF User's Guide Volume I* for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

Appendix G. Notices

This information was developed for products and services offered in the USA.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA

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

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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

IBM Corporation
Mail Station P300
2455 South Road
Poughkeepsie, NY 12601-5400
USA

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

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

This product contains code licensed from RSA Data Security Incorporated.



Programming Interface Information

This book is intended to help the installation:

- Install, maintain, or modify the RACF program product using the macros provided by RACF.
- Code the interfaces used to invoke RACF using the RACF ISPF panels.

This publication primarily documents intended programming interfaces that allow the installation to write programs to obtain the services of RACF.

This publication also documents information that is NOT intended to be used as programming interfaces of RACF. This information is identified where it occurs, either by an introductory statement to a chapter or section or by the following marking:

————— **NOT programming interface information** —————

————— **End of NOT programming interface information** —————

Trademarks

The following terms are trademarks of IBM Corporation in the United States or other countries or both:

BookManager
CICS

CICS/ESA
DB2
DFSMSdss
eServer
Hiperbatch
IBM
IBMLink
IMS
Language Environment
Library Reader
MVS
MVS/SP
OpenEdition
OS/390
RACF
Redbooks
Resource Link
S/390
SecureWay
SQL/DS
System/390
SystemView
TalkLink
VM/ESA
VTAM
z/Architecture
z/OS
z/OS.e
z/VM
zSeries

Lotus and Lotus Notes are trademarks of Lotus Development Corporation in the United States, other countries, or both.

Tivoli, TME, and NetView are trademarks of International Business Machines Corporation or Tivoli Systems, Inc. in the United States, other countries, or both.

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

Other company, product, or service names may be trademarks or service marks of others.

RACF Glossary

This glossary defines technical terms and abbreviations used in RACF documentation. If you do not find the term you are looking for, refer to the index of the appropriate RACF manual or view *IBM Glossary of Computing Terms*, available from: <http://www.ibm.com/ibm/terminology>

Sequence of Entries

For purposes of clarity and consistency of style, this glossary arranges the entries alphabetically on a letter-by-letter basis, which means:

- Only the letters of the alphabet are used to determine sequence, and
- Special characters and spaces between words are ignored.

Organization of Entries

Each entry consists of:

- A single-word term,
- A multiple-word term,
- An abbreviation for a term, or
- An acronym for a term.

This entry is followed by a commentary, which includes one or more items (definitions or references) and is organized as follows:

1. An item number, if the commentary contains two or more items.
2. A usage label, indicating the area of application of the term, for example, "In programming," or "In TCP/IP." Absence of a usage label implies that the term is generally applicable to IBM, or to data processing.
3. A descriptive phrase, stating the basic meaning of the term. The descriptive phrase is assumed to be preceded by "the term is defined as...". The part of speech being defined is indicated by the opening words of the descriptive phrase: "To ..." indicates a verb, and "Pertaining to ..." indicates a modifier. Any other wording indicates a noun or noun phrase.
4. Annotative sentences, providing additional or explanatory information.
5. References, pointing to other entries or items in the dictionary.

References

The following cross-references are used in this glossary:

- **Contrast with:** This refers to a term that has an opposed or substantively different meaning.
- **See:** This refers the reader to (a) a related term, (b) a term that is the expanded form of an abbreviation or acronym, or (c) a synonym or more preferred term.
- **Synonym for:** This indicates that the term has the same meaning as a preferred term, which is defined in its proper place in the glossary.
- **Synonymous with:** This is a reference from a defined term to all other terms that have the same meaning.
- **Obsolete term for:** This indicates that the term should not be used and refers the reader to the preferred term.

Selection of Terms

A term is the word or group of words being defined. In this glossary, the singular form of the noun and the infinitive form of the verb are the terms most often selected to be defined. If the term has an acronym or abbreviation, it is given in parentheses immediately following the term. The abbreviation's definition serves as a pointer to the term it abbreviates, and the acronym's definition serves as a pointer to the term it represents.

A

access. The ability to use a protected resource.

access authority. (1) The privileges granted to a particular user or group when accessing a protected resource (such as the ability to read or to update a data set). For resources protected by RACF profiles, the access authorities are NONE, EXECUTE, READ, UPDATE, CONTROL, and ALTER. These authorities are hierarchical, with READ also granting EXECUTE, UPDATE granting READ, and so forth. (2) RACF also has access authorities of READ, WRITE, and EXECUTE (or SEARCH) when dealing with files and directories in the HFS. Note that these authorities are not hierarchical, and HFS files are not protected by RACF profiles, although they do have access authorities.

access ACL. An ACL that is used to provide protection for a file system object.

Glossary

access control. In computer security, ensuring that the resources of a computer system can be accessed only by authorized users in authorized ways.

access control list (ACL). (1) In computer security, a collection of all access rights for one object. In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights; for example, a list associated with a file that identifies users who can access the file and identifies their access rights to that file. (2) In z/OS UNIX, an extension to the base POSIX permission bits. Similar to the access list of a RACF profile, an ACL for a file system object contains entries that specify access permissions for individual users and groups.

ACL. See access control list.

access list. Synonym for *standard access list*. Contrast with *conditional access list*.

ACEE. (accessor environment element) A control block that contains a description of the current user's security environment, including user ID, current connect group, user attributes, and group authorities. An ACEE is constructed during user identification and verification. See *ENVR object*.

ADAU. See *automatic direction of application updates*.

ADSP. See *automatic data set protection*.

ADSP attribute. A user attribute that establishes an environment in which all permanent DASD data sets created by the user are automatically defined to RACF and protected with a discrete profile. See *automatic data set protection*.

Advanced Program-to-Program Communication (APPC). A set of interprogram communication services that support cooperative transaction processing in an SNA network. APPC is the implementation, on a given system, of SNA's LU type 6.2. See *LU type 6.2* and *APPC/MVS*.

| **AIM.** See *application identity mapping (AIM)*.

APF-authorized. A type of system authorization using the authorized program facility (APF) that allows an installation to identify system or user programs that can use sensitive system functions. To maintain system security and integrity, a program must be authorized by the APF before it can access restricted functions, such as supervisor calls (SVC) or SVC paths.

API. See *application programming interface*.

APPC. See *Advanced Program-to-Program Communication*.

APPC application. See *transaction program (TP)*.

APPC/MVS. The implementation of SNA's LU 6.2 and related communication services in the MVS base control program.

| **application identity mapping (AIM).** Allows mapping between RACF user IDs and various application identities, such as those associated with z/OS UNIX, Novell Directory Services, and Lotus Notes.

application programming interface (API). A software interface that enables applications to communicate with each other. An API is the set of programming language constructs or statements that can be coded in an application program to obtain the specific functions and services provided by an underlying operating system or service program.

application user identity. An alternate name by which a RACF user can be known to an application.

appropriate privileges. Describes which users can perform an action (such as execute a command, issue a syscall, and so forth) in a UNIX environment. Usually refers to having superuser authority or an appropriate subset of superuser authority.

attribute. See *user attribute* and *group-related user attribute*.

AUDIT request. The issuing of the RACROUTE macro with REQUEST=AUDIT specified. An AUDIT request is a general-purpose security request that a resource manager can use to audit.

AUDITOR attribute. A user attribute that allows the user to specify logging options on the RACF commands and list any profile (including its auditing options) using the RACF commands. Contrast with *group-AUDITOR attribute*.

AUTH request. The issuing of the RACROUTE macro with REQUEST=AUTH specified. The primary function of an AUTH request is to check a user's authorization to a RACF-protected resource or function. The AUTH request replaces the RACHECK function. See *authorization checking*.

authentication. (1) Verification of the identity of a user or the user's eligibility to access an object. (2) Verification that a message has not been altered or corrupted. (3) A process used to verify the user of an information system or protected resources. See also *password*.

authority. The right to access objects, resources, or functions. See *access authority*, *class authority*, and *group authority*.

authorization checking. The action of determining whether a user is permitted access to a protected resource. Authorization checking refers to the use of RACROUTE REQUEST=AUTH, RACROUTE REQUEST=FASTAUTH, or any of the RACF callable

services unless otherwise stated. Note, however, that other RACF functions can also perform authorization checking as a part of their processing. For example, RACROUTE REQUEST=VERIFY can also check a user's authority to use a terminal or application.

automatic command direction. An RRSF function that enables RACF to automatically direct certain commands to one or more remote nodes after running the commands on the issuing node. Commands can be automatically directed based on who issued the command, the command name, or the profile class related to the command. Profiles in the RRSFDATA class control to which nodes commands are automatically directed. See *automatic direction of application updates*, *automatic password direction*, and *command direction*.

automatic data set protection (ADSP). A system function, enabled by the SETROPTS ADSP specification and the assignment of the ADSP attribute to a user with ADDUSER or ALTUSER, that causes all permanent data sets created by the user to be automatically defined to RACF with a discrete RACF profile.

automatic direction. See *automatic command direction*, *automatic password direction*, and *automatic direction of application updates*.

automatic direction of application updates. An RRSF function that automatically directs ICHEINTY and RACROUTE macros that update the RACF database to one or more remote systems. Profiles in the RRSFDATA class control which macros are automatically directed, and to which nodes. See *automatic command direction* and *automatic password direction*.

automatic password direction. An RRSF function that extends password synchronization and automatic command direction to cause RACF to automatically change the password for a user ID on one or more remote nodes after the password for that user ID is changed on the local node. Profiles in the RRSFDATA class control for which users and nodes passwords are automatically directed. See *password synchronization*, *automatic command direction*, and *automatic direction of application updates*.

automatic profile. A tape volume profile that RACF creates when a RACF-defined user protects a tape data set. When the last data set on the volume is deleted, RACF automatically deletes the tape volume profile. Contrast with *nonautomatic profile*.

B

backup data set. A data set in the backup RACF database. For each data set in the primary RACF database, an installation should define a corresponding backup data set. See *backup RACF database*.

backup RACF database. A RACF database that reflects the contents of the primary RACF database. Backup RACF databases may be designated in the data set name table (ICHRDSNT) or specified at IPL time. You can switch to a backup database without a re-IPL if the primary RACF database fails. See *primary RACF database*.

base ACL entry. Same as permission bits (owner, group, other). The permissions can be changed using chmod. They are not physically part of the ACL.

base segment. The portion of a RACF profile that contains the fundamental information about a user, group, or resource. The base segment contains information that is common to all applications that use the profile.

BER. This term represents the Basic Encoding Rules specified in ISO 8825 for encoding data units described in abstract syntax notation 1 (ASN.1). See also *DER*.

block update command (BLKUPD). A RACF diagnostic command used to examine or modify the content of individual physical records in a RACF data set.

C

cache structure. A coupling facility structure that contains data accessed by systems in a sysplex.

callable service. In z/OS UNIX, a request by an active process for a service. Synonymous with *syscall*.

category. See *security category*.

CDMF. See *Commercial Data Masking Facility*.

CDT. See *class descriptor table*.

certificate. See *digital certificate*.

certificate authority. An organization that issues digital certificates. The certificate authority authenticates the certificate owner's identity and the services that the owner is authorized to use, issues new certificates, renews existing certificates, and revokes certificates belonging to users who are no longer authorized to use them.

certificate-authority certificate. A type of certificate managed by RACF. See *digital certificate*.

certificate name filter. A general resource profile created by the RACDCERT MAP command that maps multiple user IDs to a digital certificate in order to simplify administration of certificates, conserve storage space in the RACF database, maintain accountability, or maintain access control granularity.

CICS. See *Customer Information Control System*.

Glossary

class. A collection of RACF-defined entities (users, groups, and resources) with similar characteristics. Classes are defined in the class descriptor table (CDT), except for the USER, GROUP, and DATASET classes.

class authority (CLAUTH). An attribute enabling a user to define RACF profiles in a class defined in the class descriptor table. A user can have class authorities to zero or more classes.

class descriptor table (CDT). A table consisting of an entry for each class except the USER, GROUP, and DATASET classes. The CDT contains the classes supplied by IBM and the installation-defined classes.

classification model 1. See *single-subsystem scope*.

classification model 2. See *multiple-subsystem scope*.

CLAUTH attribute. See *class authority*.

command direction. An RRSF function that allows a user to issue a command from one user ID and direct that command to run in the RACF address space on the same system or on a different RRSF node, using the same or a different user ID. Before a command can be directed from one user ID to another, a user ID association must be defined between them using the RACLINK command.

command prefix facility (CPF). An MVS facility that provides a registry for command prefixes. CPF ensures that two or more subsystems do not have the same or overlapping command prefixes for MVS operator commands.

Commercial Data Masking Facility (CDMF). An encryption function that uses a weaker key (40 bit) of the Data Encryption Standard (DES) algorithm. RACF uses CDMF to mask the data portion of RRSF transaction processing message packets. CDMF is part of the IBM Common Cryptographic Architecture.

common programming interface (CPI). An evolving application programming interface (API), supplying functions to meet the growing demands from different application environments and to achieve openness as an industry standard for communications programming. CPI-C provides access to interprogram services such as sending and receiving data, synchronizing processing between programs, and notifying a partner of errors in the communication.

conditional access list. The portion of a resource profile that specifies the users and groups that may access the resource at a specified level when a specified condition is true. For example, with program access to data sets, the condition is that the user must be executing the program specified in the access list. Contrast with *standard access list*.

coordinator system. In a RACF data sharing group, the system on which the system operator or administrator enters a RACF command that is propagated throughout the group. Contrast with *peer system*.

coupling facility. The hardware element that provides high-speed caching, list processing, and locking functions in a sysplex.

CPF. See *command prefix facility*.

CPI-C. See *common programming interface*.

current connect group. The group specified by a user when logging on to the system, or the user's default group if the user did not specify a group when logging on. With SETROPTS NOGRPLIST in effect, RACF uses the user's authority and this group's authority during access checking. With SETR GRPLIST in effect, RACF includes the authority of the user's other groups, if any, but the user still has only one "current connect group". You can use the &RACGPID variable in members of GLOBAL profiles to refer to the user's current connect group.

current security label. The security label that RACF uses in RACF authorization checking if the SECLABEL class is active. For interactive users, this is the security label specified when the user logged on, or (if no security label was specified) the default security label in the user's user profile. For batch jobs, this is the security label specified in the SECLABEL operand of the JOB statement, or (if no security label was specified) the user's current security label in the user profile associated with the job.

Customer Information Control System (CICS). A program licensed by IBM that provides online transaction processing services and management for critical business applications. CICS runs on many platforms (from the desktop to the mainframe) and is used in various types of networks that range in size from a few terminals to many thousands of terminals. The CICS application programming interface (API) enables programmers to port applications among the hardware and software platforms on which CICS is available. Each product in the CICS family can interface with the other products in the CICS family, thus enabling interproduct communication.

D

DASDVOL authority. A preferred alternative to assigning the OPERATIONS or group-OPERATIONS attribute, DASDVOL authority allows you to authorize operations personnel to access only those volumes that they must maintain. Using DASDVOL authority is also more efficient for functions such as volume dumping, because only one authorization check for the volume needs to be issued, instead of individual requests for each data set on the volume. Note that modern data

management software (such as DFSMSdss) does not require DASDVOL authority. Contrast with *OPERATIONS attribute*, and *group-OPERATIONS attribute*.

Data Lookaside Facility (DLF). A facility that processes DLF objects. A DLF object contains data from a single data set managed by Hiperbatch. The user (an application program) is connected to the DLF object, and the connected user can then access the data in the object through normal QSAM or VSAM macro instructions.

data security. The protection of data from intentional or unintentional unauthorized disclosure, modification, or destruction.

data security monitor (DSMON). A RACF auditing tool that produces reports enabling an installation to verify its basic system integrity and data security controls.

data set profile. A profile that provides RACF protection for one or more data sets. The information in the profile can include the data set profile name, profile owner, universal access authority, access list, and other data. See *discrete profile* and *generic profile*.

data sharing group, RACF. A collection of one or more instances of RACF in a sysplex that have been identified to XCF and assigned to the group defined for RACF sysplex data sharing. RACF joins group IRRXCF00 when enabled for sysplex communication.

data sharing mode. An operational RACF mode that is available when RACF is enabled for sysplex communication. Data sharing mode requires installation of coupling facility hardware.

DB2 administrative authority. A set of privileges, often covering a related set of objects, and often including privileges that are not explicit, have no name, and cannot be specifically granted. For example, the ability to terminate any utility job is included in the SYSOPR authority.

DB2 explicit privilege. A privilege that has a name, and is held as the result of an SQL GRANT statement.

DCE. See *Distributed Computing Environment*.

default ACL. An ACL that is specifically associated with a directory, and which gets inherited by an object created within the directory.

default group. The group specified in a user profile that provides a default current connect group for the user. See *current connect group*.

DEFINE request. The issuing of the RACROUTE macro with REQUEST=DEFINE specified or using a RACF command to add or delete a resource profile

causes a DEFINE request. The DEFINE request replaces the RACDEF function.

delegation. The act of giving users or groups the necessary authority to perform RACF operations.

DER. This term represents the Distinguished Encoding Rules, which are a subset of the Basic Encoding Rules. See also *BER*.

digital certificate. A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority.

RACF can manage three types of digital certificates:

- **Certificate-authority certificate.** A certificate associated with a certificate authority and is used to verify signatures in other certificates.
- **Site certificate.** A certificate associated with a server, or network entity other than a user or certificate authority.
- **User certificate.** A certificate associated with a RACF user ID that is used to authenticate the user's identity, and may also be used to represent a server.

DIRAUTH request. The issuing of the RACROUTE macro with REQUEST=DIRAUTH specified. A DIRAUTH request works on behalf of the message-transmission managers to ensure that the receiver of a message meets security-label authorization requirements.

directed command. A RACF command that is issued from a user ID on an RRSF node. It runs in the RACF subsystem address space on the same or a different RRSF node under the authority of the same or a different user ID. A directed command is one that specifies AT or ONLYAT. See *command direction* and *automatic command direction*.

directory default ACL. A model ACL that gets inherited by subdirectories that are created within the parent directory.

directory model ACL. See *directory default ACL*.

discrete profile. A resource profile that provides RACF protection for a single resource. Contrast with *generic profile* and *fully-qualified generic profile*.

discretionary access control. An access control environment in which the resource owner determines who can access the resource. Contrast with *mandatory access control*.

disjoint. Pertaining to security labels, when the set of security categories that defines the first does not include the set of security categories that defines the second, and the set of security categories that defines the second does not include the set of security categories that defines the first. This also means that the first does not dominate the second and the second does not dominate the first. See *dominate*.

Glossary

Distributed Computing Environment (DCE). The Open Group specification (or a product derived from this specification) that assists in networking. DCE provides such functions as authentication, directory service (DS), and remote procedure call (RPC).

DLF object. When Data Lookaside Facility (DLF) is active, the first attempt to access a QSAM or VSAM data set defined to DLF creates a DLF object. A DLF object contains data from a single data set managed by Hiperbatch. The user (an application program) is connected to the DLF object, and the connected user can then access the data in the object through normal QSAM or VSAM macro instructions.

dominate. One security label dominates a second security label when the security level that defines the first is equal to or greater than the security level that defines the second, and the set of security categories that defines the first includes the set of security categories that defines the second. A security label dominates itself since comparison of a security label with itself meets this definition.

DSMON. See *data security monitor*.

E

effective group identifier (effective GID). When the user connects to the system (for example, logs on to a TSO/E session), one group is selected as the user's current group. When a user becomes a z/OS UNIX user, the GID of the user's current group becomes the effective GID of the user's process. The user can access resources available to members of the user's effective GID. See *group identifier (GID)* and contrast with *real GID*.

effective user identifier (effective UID). When a user becomes a z/OS UNIX user, the UID from the user's RACF user profile becomes the effective UID of the user's process. The system uses the effective UID to determine if the user is a file owner. See *user identifier (UID)* and contrast with *real UID*.

EIM. See *Enterprise identity mapping*.

EIM domain. An LDAP name space that contains the enterprise identifiers, registry users, and relationships or associations between them.

Enterprise identity mapping (EIM). An infrastructure that user administration applications, servers, operating systems, and auditing tools can use to store identity mappings in a centralized, distributed registry (LDAP). The information is stored in LDAP to allow one user ID to be mapped to another (as long as the identities belong to the same application) using this support.

entity. A user, group, or resource (for example, a DASD data set) that is defined to RACF.

ENVR object. A transportable form of the ACEE that can be used within a single system to create the original ACEE without accessing the RACF database. It can be used, with limits, elsewhere in a single sysplex to recreate the original ACEE without accessing the RACF database.

equivalence. Two security labels that contain the same security level and the same set of categories are considered equivalent, with each being dominated by and dominating the other.

erase-on-scratch. The physical overwriting of data on a DASD data set when the data set is deleted (scratched).

extended ACL entry. An ACL entry for an individual user or group.

EXTRACT request. The issuing of the RACROUTE macro with REQUEST=EXTRACT specified. An EXTRACT request retrieves or replaces certain specified fields from a RACF profile or encodes certain clear-text (readable) data. The EXTRACT request replaces the RACXTRT function.

F

failsoft processing. (1) Processing that occurs when no data sets in the primary RACF database are available (RACF is installed but inactive). RACF cannot make decisions to grant or deny access. The operator is prompted frequently to grant or deny access to data sets. The resource manager decides on the action for general resource classes with a return code of 4. (2) Failsoft processing can also occur as the result of RVAR Y INACTIVE (temporary failsoft) or as the result of a serious system error requiring a re-IPL (permanent failsoft).

FASTAUTH request. The issuing of the RACROUTE macro with REQUEST=FASTAUTH specified. The primary function of a FASTAUTH request is to check a user's authorization to a RACF-protected resource or function. A FASTAUTH request uses only in-storage profiles (brought into storage using RACF functions such as RACROUTE REQUEST=LIST) for faster performance than an AUTH request. The FASTAUTH request replaces the FRACHECK function. See *authorization checking*.

field-level access checking. The RACF facility by which a security administrator can control access to segments, other than the base segment, in a RACF profile and fields in those segments.

file default ACL. A model ACL that is inherited by files that are created within the parent directory.

file model ACL. See file default ACL.

file permission bits. In z/OS UNIX, information about a file that is used, along with other information, to determine if a process has read, write, or execute/search permission to a file or directory. The bits are divided into three parts, which are owner, group, and other.

file security packet (FSP). In z/OS UNIX, a control block containing the security data (file's owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

file system object. Used to generically refer to either a file or directory.

file transfer protocol (FTP). In the Internet suite of TCP/IP-related protocols, an application-layer protocol that transfers bulk-data files between machines or hosts.

FMID. See *function modification identifier*.

FRACHECK request. RACROUTE REQUEST=FASTAUTH replaces the FRACHECK function. See *FASTAUTH request*.

FSP. See *file security packet*.

FTP. See *File Transfer Protocol*.

fully-qualified generic profile. A DATASET profile that was defined using the GENERIC operand and has a name that contains no generic characters. A fully-qualified generic profile protects only resources whose names exactly match the name of the profile. Contrast with *discrete profile* and *generic profile*.

function modification identifier (FMID). A 7-character identifier that is used in elements associated with z/OS and OS/390 to identify the release of the element.

G

GDG. See *generation data group*.

general resource. Any resource, other than an MVS data set, that is defined in the class descriptor table (CDT). General resources include DASD volumes, tape volumes, load modules, terminals, IMS and CICS transactions, and installation-defined resource classes.

general resource profile. A profile that provides RACF protection for one or more general resources. The information in the profile can include the general resource profile name, profile owner, universal access authority, access list, and other data.

general user. A user who has limited RACF privileges, such as logging on, accessing resources, and creating data sets. General users typically use and create

RACF-protected resources, but have no authority to administer resources other than their own.

generation data group (GDG). A collection of data sets with the same base name, such as PAYROLL, that are kept in chronological order. Each data set in the GDG is called a generation data set, and has a name such as PAYROLL.G0001V00, PAYROLL.G0002V00, and so forth.

generic profile. A resource profile that can provide RACF protection for zero or more resources. The resources protected by a generic profile have similar names and identical security requirements, though with RACFVARS, a generic profile can protect resources with dissimilar names, too. For example, a generic data set profile can protect one or more data sets. Contrast with *discrete profile*.

global access checking. The ability to allow an installation to establish an in-storage table of default values for authorization levels for selected resources. RACF refers to this table before performing normal RACROUTE REQUEST=AUTH processing and grants the request without performing an AUTH request if the requested access authority does not exceed the global value. RACF uses this table to process AUTH requests faster and with less overhead (no checking of access lists, no auditing) when you have resources for which you decide to grant access to all users, except those with restricted user IDs. If the requested access does not exceed the access granted by the table, RACF bypasses most of its normal AUTH processing. Global access checking can grant the user access to the resource, but it cannot deny access.

global resource serialization. A mechanism using ENQ with the SYSTEMS option (or, in some older programs, the RESERVE option) to serialize resources across multiple z/OS or OS/390 images. It is used by RACF to serialize access to its database and to in-storage tables and buffers.

globally RACLISTed profiles. In-storage profiles for RACF-defined resources that are created by RACROUTE REQUEST=LIST and that are anchored from an ACEE. Globally RACLISTed in-storage profiles are shared across a system, such as the way that in-storage profiles created by SETROPTS RACLIST are shared. Contrast with *locally RACLISTed profiles*.

group. A collection of RACF-defined users who can share access authorities for protected resources.

group-ADSP attribute. A group-related user attribute similar to the ADSP attribute for a user, but assigned by using the CONNECT command to restrict its effect to those cases where the user creates data sets with that group as the high level qualifier of the data set name (or as determined by the naming convention table or exit).

group-AUDITOR attribute. A group-related user attribute similar to the AUDITOR attribute for a user, but

Glossary

assigned by using the **CONNECT** command to restrict the user's authority to resources that are within the scope of the group. Contrast with *AUDITOR attribute*.

group authority. An authority specifying which functions a user can perform in a group. The group authorities are **USE**, **CREATE**, **CONNECT**, and **JOIN**.

group data set. A RACF-protected data set in which either the high-level qualifier of the data set name or the qualifier supplied by an installation-naming convention table or exit routine is a RACF group name.

group-GRPACC attribute. A group-related user attribute similar to the **GRPACC** attribute for a user, but assigned by using the **CONNECT** command to restrict its effect to the specific group. Contrast with *GRPACC attribute*.

group ID. Obsolete term for *group name*.

group identifier (GID). A number between 0 and 2 147 483 647 that identifies a group of users to z/OS UNIX. The GID is associated with a RACF group name when it is specified in the OMVS segment of the group profile. See *real GID*. Contrast with *effective group identifier (effective GID)*.

group name. A string of 1–8 characters that identifies a group to RACF. The first character must be A through Z, # (X'7B'), \$ (X'5B'), or @ (X'7C'). The rest can be A through Z, #, \$, @, or 0 through 9.

group-OPERATIONS attribute. (1) A group-related user attribute similar to the **OPERATIONS** attribute for a user, but assigned by using the **CONNECT** command to restrict its effect to those resources that are within the scope of the group. (2) If a person needs to perform maintenance activities on DASD volumes, it is more efficient (for RACF processing) and better (for limiting the resources the person can access) to give the person authority to those volumes using the **PERMIT** command than to assign the person the **OPERATIONS** or **group-OPERATIONS** attribute. Contrast with *DASDVOL authority* and *OPERATIONS attribute*.

group profile. A profile that defines a group. The information in the profile includes the group name, profile owner, and users in the group.

grouping profile. A profile in a resource group class.

group-related user attribute. A user attribute, assigned at the group level, that enables the user to control the resource, group, and user profiles associated with the group and its subgroups. Group-related user attributes include **group-SPECIAL** attribute, **group-AUDITOR** attribute, and **group-OPERATIONS** attribute. Contrast with *user attribute*.

group-REVOKE attribute. Assigned through the **CONNECT** command that prevents the user from using

that group as the current connect group. Also prevents RACF from considering that group during authorization checking.

group-SPECIAL attribute. A group-related user attribute similar to the **SPECIAL** user attribute, but it is assigned by the **CONNECT** command to restrict the user's authority to users, groups, and resources within the scope of the group. Within this scope, it gives the user full control over everything except auditing options. However, it does not give the user authority to change global RACF options that will affect processing outside the group's scope. Contrast with *SPECIAL attribute*.

GRPACC attribute. With this attribute, any group data sets that the user defines to RACF (through the **ADSP** attribute, the **PROTECT** operand on the **DD** statement, or the **ADDSD** command) are automatically made accessible to other users in the group at the **UPDATE** level of access authority if the user defining the profile is a member of the group. Contrast with *group-GRPACC attribute*.

H

HFS. See *hierarchical file system*.

hierarchical file system (HFS). The file system for z/OS UNIX that organizes data in a tree-like structure of directories.

I

ICB. See *inventory control block*.

| **ICL.** See *Issued certificate list (ICL)*.

ICHRIN03. See *started procedures table*.

inheritance. The act of automatically associating an ACL with a newly created object without requiring administrative action.

| **Issued certificate list (ICL).** PKI Services database containing the history of issued certificates.

interprocess communication facilities (IPC). IPC facilities are services that allow different processes to communicate. Message passing (using message queues), semaphore sets, and shared memory services are forms of interprocess communication facilities.

inventory control block (ICB). The first block in a RACF database. The ICB contains a general description of the database and, for the master primary data set, holds the RACF global options specified by **SETROPTS**.

IPC. See *interprocess communication facilities*.

issuer's distinguished name (IDN). The X.509 name that is associated with a certificate authority.

K

kernel. The part of z/OS UNIX that provides support for such services as UNIX I/O, process management, and general UNIX functionality.

kernel address space. The address space in which the z/OS UNIX kernel runs. See *kernel*.

key. In cryptography, a sequence of symbols that is used with a cryptographic algorithm for encrypting or decrypting data. See *private key* and *public key*.

key ring. A named collection of certificates for a specific user or server application used to determine the trustworthiness of a client or peer entity.

L

label. A usable "handle" for a certificate.

LDAP. See *Lightweight directory access protocol*.

Lightweight access directory protocol (LDAP). Similar to directory access protocol (DAP), but simpler to use and has a programming interface; LDAP is composed of entries identified by their distinguished names.

link pack area (LPA). An area of virtual storage containing reenterable routines from system libraries that are loaded at IPL time and can be used concurrently by all tasks in the system. The LPA presence in main storage saves loading time.

LIST request. The issuing of the RACROUTE macro with REQUEST=LIST specified. A LIST request builds in-storage profiles for a RACF general resource class. The LIST request replaces the RACLIST function.

list-of-groups checking. A RACF option (SETROPTS GRPLIST) that enables a user to access all resources available to all groups of which the user is a nonrevoked member, regardless of the user's current connect group. For any particular resource, RACF allows access based on the highest access among the groups in which the user is a member.

local logical unit (local LU). A logical unit that resides on the local system. Contrast with *partner logical unit (partner LU)*, or *remote logical unit (remote LU)*, which typically resides on a remote system. When both the local and partner LUs reside on the same system, the LU through which communication is initiated is the local LU, and the LU through which communication is received is the partner LU.

local mode. An RRSF node is operating in local mode when it has no RRSF logical node connection with any other RRSF node.

local transaction program (local TP). A transaction program that resides on the local system. Contrast with *partner transaction program (partner TP)*, which typically resides on a remote system.

locally RACLISTed profiles. In-storage profiles for RACF-defined resources that are created by RACROUTE REQUEST=LIST and that are anchored from an ACEE. Locally RACLISTed in-storage profiles are not shared across a system, the way that in-storage profiles created by SETROPTS RACLIST are shared. Contrast with *globally RACLISTed profiles*.

logging. The recording of audit data about specific events.

logical connection. See *RRSF logical node connection*.

logical unit (LU). A type of network accessible unit that enables users to gain access to network resources and communicate with each other.

logical unit type 6.2 (LU type 6.2). The SNA logical unit type that supports general communication between programs in a cooperative processing environment. Also, the SNA logical unit type on which CPI-C and APPC/MVS TP conversation services are built.

LPA. See *link pack area*.

LU. See *logical unit*.

LU type 6.2. See *logical unit type 6.2*.

M

MAC. See *mandatory access control*.

main system. The system on a multisystem RRSF node that is designated to receive most of the RRSF communications sent to the node.

managed user ID association. A user ID association in which one of the associated user IDs is a managing user ID, and the other is a managed user ID. The managing user ID can run allowed RACF commands under the authority of the managed user ID. The managed user ID cannot run commands under the authority of the managing user ID. A managed user ID association does not allow password synchronization between the associated user IDs. Contrast with *peer user ID association*.

mandatory access control (MAC). A means of restricting access to objects on the basis of the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (clearance) of subjects to access information of such sensitivity.

Glossary

mask. A technique to provide protection against casual viewing of a password that has been defined or altered, when an encryption function is not available.

master primary data set. The first data set activated in the primary RACF database.

MCS. See *multiple console support*.

MCS console. A non-SNA device defined to MVS that is locally attached to an MVS system and is used to enter commands and receive messages.

member. A user belonging to a group.

member profile. A profile that defines a member and security level for that member.

member system. Any one of the MVS system images in a multisystem RRSF node.

model ACL. See default ACL.

modeling. See *profile modeling*.

multiple console support (MCS). The operator interface in an MVS system.

multiple-subsystem scope. A RACF classification model used in conjunction with the RACF/DB2 external security module to construct DB2 resource names. Default for the highest-level qualifier is the DB2 subsystem or group name.

multisystem node. See *multisystem RRSF node*.

multisystem RRSF node. An RRSF node consisting of multiple MVS system images that share the same RACF database. One of the systems is designated to be the main system, and it receives the unsolicited RRSF communications sent to the node.

multi-subsystem scope. A classification model used in conjunction with the RACF/DB2 external security module to construct DB2 classes with the subsystem ID as part of the class name. Contrast with *single-subsystem scope*.

MVS. (multiple virtual storage) The mainframe operating system that allows multiple users to work simultaneously using the full amount of virtual storage.

N

NCSC. National Computer Security Center. The part of the U.S. Department of Defense that determines defense and security criteria.

network-qualified name. An identifier for a partner LU in the form *netid.luname*, where *netid* is a 1–8 character network identifier and *luname* is a 1–8 character LU name.

node. See *RRSF node*.

nonautomatic profile. A tape volume profile that RACF creates when an RDEFINE command is issued or when tape data set protection is not active. A tape volume profile created in this manner is called a nonautomatic profile because RACF never deletes the profile except in response to the RDELETE command. Contrast with *automatic profile*.

non-data sharing mode. One of two normal modes of operation when RACF is enabled for sysplex communication and is the mode in which RACF communicates information using sysplex facilities to other instances of RACF, but does not make use of the coupling facility in doing so.

O

OpenExtensions VM. A feature of VM systems that provides a set of UNIX-based programming interfaces, such as shells and utilities, in support of selected POSIX and X/OPEN portability guide (XPG) standards.

OPERATIONS attribute. A user attribute that grants the equivalent of ALTER access to all data sets unless the user or one of the user's connect groups appears explicitly in the access list of a data set's profile. If a user needs to perform maintenance activities on DASD volumes, granting DASDVOL authority to those volumes using the PERMIT command is preferred over assigning the OPERATIONS or group-OPERATIONS attribute. Note that most modern DASD maintenance programs do not require the OPERATIONS attribute. Contrast with *DASDVOL authority* and *group-OPERATIONS attribute*.

operator identification card (OIDCARD). A small card with a magnetic stripe encoded with unique characters and used to verify the identity of a terminal operator to RACF.

OS/390. A program licensed by IBM that not only includes and integrates functions previously provided by many IBM software products, including the MVS operating system, but also:

1. Is an open, secure operating system for the IBM S/390 family of enterprise servers
2. Complies with industry standards
3. Is Year 2000 ready and enabled for network computing and e-business
4. Supports technology advances in networking server capability, parallel processing, and object-oriented programming

OS/390 UNIX group identifier (GID). See *group identifier (GID)*.

OS/390 UNIX System Services (OS/390 UNIX). The set of functions provided by the shells, utilities, kernel, file system, debugger, Language Environment, and

other elements of the OS/390 operating system that allows users to write and run application programs that conform to UNIX standards.

OS/390 UNIX user identifier (UID). See *user identifier (UID)*.

owner. The user or group that creates a profile, or is specified as the owner of a profile. The owner can modify, list, or delete the profile.

P

PADS. See *program access to data sets (PADS)*.

partner logical unit (partner LU). A logical unit that typically resides on a remote system. Often synonymous with *remote logical unit (remote LU)*. Contrast with *local logical unit (local LU)*, which resides on the local system. When both the local and partner LUs reside on the same system, the LU through which communication is initiated is the local LU, and the LU through which communication is received is the partner LU.

partner transaction program (partner TP). A transaction program that resides on a remote system. Contrast with *local transaction program (local TP)*, which typically resides on the local system.

PassTicket. An alternative to the RACF password that permits workstations and client machines to communicate with the host. It allows a user to gain access to the host system without sending the RACF password across the network.

password. A string of characters known to a user who must specify it to gain full or limited access to a system and to the data stored within it. RACF uses a password to verify the identity of the user.

password synchronization. An option that can be specified when a peer user ID association is defined between two user IDs. If password synchronization is specified for a user ID association, then whenever the password for one of the associated user IDs is changed, the password for the other user ID is automatically changed to the newly defined password. See *automatic password direction*.

peer system. In a RACF data sharing group, any system to which RACF propagates a command entered by the system operator or administrator. Contrast with *coordinator system*.

peer user ID association. A user ID association that allows either user ID to run allowed RACF commands under the authority of the other user ID using command direction. A peer user ID association can also establish password synchronization between the associated user IDs. Contrast with *managed user ID association*.

permission bits. In z/OS UNIX, part of security controls for directories and files stored in the hierarchical file system (HFS). Used to grant read, write, search (just directories), or execute (just files) access to owner, file or directory owning group, or all others.

persistent verification (PV). A VTAM security option for conversation-level security between two logical units (LUs) that provides a way of reducing the number of password transmissions by eliminating the need to provide a user ID and password on each attach (allocate) during multiple conversations between a user and a partner LU. The user is verified during the signon process and remains verified until the user has been signed off the partner LU.

| **PKCS.** See *Public key cryptographic standards*.

| **PKI.** See *Public key infrastructure*.

| **PKIX.** See *Public key infrastructure standards*.

POSIT. A number specified for each class in the class descriptor table that identifies a set of flags that control RACF processing options.

POSIX. (Portable Operating System Interface For Computer Environments) An IEEE standard for computer operating systems.

primary data set. A data set in the primary RACF database. See *master primary data set*.

primary RACF database. The RACF database designated in the data set name table (ICHRDSNT), or specified at IPL time, that contains the RACF profiles used for authorization checking. The primary RACF database may consist of as many as 90 data sets. See *backup RACF database*.

private key. In public key cryptography, a key that is known only to its owner. Contrast with *public key*.

problem state. A state during which a processing unit cannot execute input/output and other privileged instructions. Contrast with *supervisor state*.

process. In z/OS UNIX, a function created by a **fork()** request. See *task*.

profile. Data that describes the significant characteristics of a user, a group of users, or one or more computer resources. A profile contains a base segment, and optionally, a number of other segments. See *data set profile*, *discrete profile*, *general resource profile*, *generic profile*, *group profile*, and *user profile*.

profile list. A list of profiles indexed by class (for general resources) or by the high-level qualifier (for data set profiles) and built in storage by the RACF routines.

profile modeling. The ability for a user or an installation to copy information (such as universal access authority or access lists) from an existing

Glossary

resource profile when defining a new resource profile. This might occur automatically when using ADDSD based on the MODEL specification in a USER or group PROFILE, or manually with the FROM keyword of the ADDSD and RDEFINE commands, or with keywords on RACROUTE REQUEST=DEFINE.

program access to data sets (PADS). A RACF function that enables an authorized user or group of users to access one or more data sets at a specified access authority only while running a specified RACF-controlled program. See *program control*.

program control. A RACF function that enables an installation to control who can run RACF-controlled programs. See *program access to data sets*.

protected resource. A resource defined to RACF for the purpose of controlling access to the resource. Some of the resources that can be protected by RACF are DASD volumes, tape volumes, load modules, terminals, IMS and CICS transactions, and installation-defined resource classes.

protected user ID. A user ID that cannot enter the system by any means that requires a password, and cannot be revoked by invalid password attempts. Assigning a protected user ID to z/OS UNIX, a UNIX daemon, or another important started task or subsystem assures that the ID cannot be used for other purposes, and that functions will not fail because the ID has been revoked.

public key. In public key cryptography, a key that is made available to everyone. Contrast with *private key*.

public key cryptography. Cryptography in which public keys and private keys are used for encryption and decryption. One party uses a common public key and the other party uses secret private key. The keys are complementary in that if one is used to encrypt data, the other can be used to decrypt it.

| **Public key cryptographic standards (PKCS).** Set of
| standards developed by RSA Corporation to facilitate
| interoperability for cryptographic protocols.

| **Public key infrastructure (PKI).** The set of hardware,
| software, people, policies, and procedures needed to
| create, manage, store, distribute, and revoke public key
| certificates based on public key cryptography.

| **Public key infrastructure Standards (PKIX).** Set of
| standards needed to support an X.509-based PKI.

PV. See *persistent verification*.

R

RACDEF request. The DEFINE function replaces the RACDEF function. See *DEFINE request*.

RACF. See *Resource Access Control Facility*.

RACF/DB2 external security module. A RACF exit point that receives control from the DB2 access control authorization exit point (DSNX@XAC) to handle DB2 authorization checks.

RACF database. The repository for the security information that RACF maintains.

RACF data set. One of the data sets comprising the RACF database.

RACF-indicated. Pertaining to a data set for which the RACF indicator is set on. If a data set is RACF-indicated, a user can access the data set only if a RACF profile or an entry in the global access checking table exists for that data set. On a system without RACF, a user cannot access a RACF-indicated data set until the indicator is turned off. For VSAM data sets, the indicator is in the catalog entry. For non-VSAM data sets, the indicator is in the data set control block (DSCB). For data sets on tape, the indicator is in the RACF tape volume profile of the volume that contains the data set.

RACF manager. The routines within RACF that provide access to the RACF database. Contrast with *RACF storage manager*.

RACF-protected. Pertaining to a resource that has either a discrete profile or an applicable generic profile. A data set that is RACF-protected by a discrete profile must also be RACF-indicated.

RACF remote sharing facility (RRSF). RACF services that function within the RACF subsystem address space to provide network capabilities to RACF.

RACF remove ID utility. A RACF utility that identifies references to user IDs and group names in the RACF database. The utility can be used to find references to residual user IDs and group names or specified user IDs and group names. The output from this utility is a set of RACF commands that can be used to remove the references from the RACF database after review and possible modification. See *residual user ID*.

RACF report writer. A RACF function that produces reports on system use and resource use from information found in the RACF SMF records. However, the preferred method for producing RACF SMF reports is the RACF SMF data unload utility (IRRADU00).

RACF segment. Obsolete term for *base segment*.

RACF SMF data unload utility (IRRADU00). A RACF utility that enables installations to create a sequential file from the security-relevant audit data. The sequential file can be viewed directly, used as input for installation-written programs, and manipulated with sort/merge utilities. It can also be uploaded to a database manager (such as DB2) to process complex inquiries and create installation-tailored reports. See *SMF records*.

RACF storage manager. Manages the allocation of storage for the RACF programs running on a system.

RACHECK request. The AUTH request replaces the RACHECK function. See *AUTH request*.

RACINIT request. The VERIFY request replaces the RACINIT function. See *VERIFY request*.

RACLIST request. The LIST request replaces the RACLIST function. See *LIST request*.

RACLISTed profiles. See *locally RACLISTed profiles* and *globally RACLISTed profiles*.

RACROUTE macro. An assembler macro that provides a means of calling RACF to provide security functions, including the *AUDIT request*, *AUTH request*, *DEFINE request*, *DIRAUTH request*, *EXTRACT request*, *FASTAUTH request*, *LIST request*, *SIGNON request*, *STAT request*, *TOKENBLD request*, *TOKENMAP request*, *TOKENXTR request*, *VERIFY request*, and *VERIFYX request*.

RACSTAT request. The STAT request replaces the RACSTAT function. See *STAT request*.

RACXTRT request. The EXTRACT request replaces the RACXTRT function. See *EXTRACT request*.

RBA. See *relative byte address*.

read-only mode. A recovery mode of operation when RACF is enabled for sysplex communication. Read-only mode does not allow updates to be made to the RACF database except for statistics generated during logon and job initiation.

real GID. The attribute of a process that, at the time of process creation, identifies the group of the user who created the process. See *group identifier (GID)*. Contrast with *effective group identifier (effective GID)*.

real UID. The attribute of a process that, at the time of process creation, identifies the user who created the process. See *user identifier (UID)*. Contrast with *effective user identifier (effective UID)*.

relative byte address (RBA). The address in the RACF database.

relative distinguished name (RDN). One component of a distinguished name.

remote logical unit (remote LU). A logical unit that resides on a remote system. Often synonymous with *partner logical unit (partner LU)*. Contrast with *local logical unit (local LU)*, which typically resides on the local system.

residual authority. References in the RACF database to group names and user IDs that have been deleted.

residual group name. References in the RACF database to a group name that has been deleted.

residual user ID. References in the RACF database to a user ID that has been deleted.

Resource Access Control Facility (RACF). A program (licensed by IBM) that provides access control by identifying and verifying the users to the system, authorizing access to protected resources, logging detected unauthorized attempts to enter the system, logging unauthorized attempts to enter the system, and logging detected accesses to protected resources. RACF is included in the Security Server and is also available as a separate program for the MVS and VM environments.

resource group profile. A general resource profile in a resource grouping class. A resource group profile can provide RACF protection for one or more resources with *unlike* names. See *resource grouping class*.

resource grouping class. A RACF class in which resource group profiles can be defined. A resource grouping class is related to another class, sometimes called a *member class*. For example, the resource grouping class GTERMINL is related to the class TERMINAL. See *resource group profile*.

resource profile. A profile that provides RACF protection for one or more resources. USER, GROUP, and CONNECT profiles are not resource profiles. The information in a resource profile can include the profile name, profile owner, universal access authority, access list, and other data. Resource profiles can be discrete profiles or generic profiles. See *discrete profile* and *generic profile*.

RESTRICTED attribute. A user attribute that can be assigned to a shared user ID, such as PUBLIC or ANONYMOS, or a user ID used with a certificate name filter, to prevent the user ID from being used to access protected resources it is not specifically authorized to access. Restricted users cannot gain access to protected resources through global access checking, UACC, or an ID(*) entry on the access list, and optionally, to a z/OS UNIX file system object through the 'other' bits.

REVOKE attribute. A user attribute that prevents a RACF-defined user from entering the system.

role. In Tivoli products, a functional grouping of user authorizations. A ROLE profile represents a role and identifies the authorizations associated with that role.

RRSF. See *RACF remote sharing facility*.

RRSF logical node connection. Two RRSF nodes are logically connected when they are properly configured to communicate through APPC/MVS, and

Glossary

they have each been configured by the TARGET command to have an OPERATIVE connection to the other.

RRSF network. Two or more RRSF nodes that have established RRSF logical node connections to each other.

RRSF node. An MVS system image or a group of MVS system images sharing a RACF database, which has been defined as an RRSF node, single-system RRSF node, or multisystem RRSF node to RACF by a TARGET command. See *RRSF logical node connection*.

RTOKEN. The RACF resource security token. An RTOKEN is an encapsulation or representation of the security characteristics of a resource. Resource managers, for example JES, can assign RTOKENs to the resources they manage; for example, JES spool files. See *UTOKEN* and *STOKEN*.

S

SAF. See *System Authorization Facility*.

secured signon. A RACF function providing an alternative to the RACF password and also providing enhanced security across a network.

security. See *data security*.

security category. An installation-defined name corresponding to a department or area within an organization whose members have similar security requirements.

security classification. The use of security categories, a security level, or both, to impose additional access controls on sensitive resources. An alternative way to provide security classifications is to use security labels.

security label. An installation-defined name that corresponds to a specific RACF security level with a set of zero or more security categories. This is equivalent to the NCSC term *sensitivity label*.

security level. An installation-defined name that corresponds to a numerical security level; the higher the number, the higher the security level.

Security Server. A licensed feature of z/OS that is comprised of Resource Access Control Facility (RACF), DCE Security Server, Lightweight Directory Access Protocol (LDAP) Server, z/OS Firewall Technologies, Open Cryptographic Enhanced Plug-ins (OCEP), and Network Authentication Service.

security token. A collection of identifying and security information that represents data to be accessed, a user, or a job. This contains a user ID, group name, security label, node of origin, and other information.

segment. A portion of a profile. The format of each segment is defined by a template.

SETROPTS RACLISTed profiles. See *globally RACLISTed profiles*.

SFS. See *Shared File System*.

| **shared GID.** An OMVS GID value that has been
| assigned to more than one group.

| **shared UID.** An OMVS UID value that has been
| assigned to more than one user.

shared file system (SFS). On VM/ESA, a part of CMS that lets users organize their files into groups known as directories and selectively share those files and directories with other users.

signed-on-from list. A list of user entries identifying those users who have been signed on from a partner LU to a local LU and is associated with persistent verification.

SIGNON request. The issuing of the RACROUTE macro with REQUEST=SIGNON specified. A SIGNON request is used to manage the signed-on-from lists associated with persistent verification.

single-subsystem scope. A classification model used in conjunction with the RACF/DB2 external security module to construct DB2 classes with the subsystem ID as part of the class name. Contrast with *multi-subsystem scope*.

single-system node. See *single-system RRSF node*.

single-system RRSF node. An RRSF node consisting of one MVS system image.

site certificate. A type of certificate managed by RACF. See *digital certificate*.

SMF. See *System Management Facility*.

SMF data unload utility. See *RACF SMF data unload utility*.

SMF records. (1) Records and system or job-related information collected by the System Management Facility (SMF) and used in billing users, reporting reliability, analyzing the configuration, scheduling jobs, summarizing direct access volume activity, evaluating data set activity, profiling system resource use, and maintaining system security. (2) Variable-length process or status records from the SMF data set that are written to the SMF log data set. These records vary in layout based on the type of system information they contain. See *RACF SMF data unload utility*.

SMS. See *Storage Management Subsystem*.

SNA. See *System Network Architecture (SNA)*.

source user ID. The source half of a source user ID and target user ID pair that has an established user ID association between them. For command direction the source user ID is the user ID that issued the command that is being directed. For password synchronization the source user ID is the user ID whose password changed, causing a change to the password of the target user ID. Contrast with *target user ID*.

SPECIAL attribute. A user attribute that gives the user full control over all of the RACF profiles in the RACF database and allows the user to issue all RACF commands, except for commands and operands related to auditing. Contrast with *group-SPECIAL attribute*.

split database. A RACF database that has been divided among multiple data sets.

standard access list. The portion of a resource profile that specifies the users and groups that may access the resource and the level of access granted to each. Synonymous with *access list*. Contrast with *conditional access list*.

started procedures table (ICHRIN03). Associates the names of started procedures with specific RACF user IDs and group names. It can also contain a generic entry that assigns a user ID or group name to any started task that does not have a matching entry in the table. However, it is recommended that you use the STARTED class for most cases rather than the started procedures table.

STAT request. The issuing of the RACROUTE macro with REQUEST=STAT specified. A STAT request determines if RACF is active and (optionally) if a given resource class is defined to RACF and active. The STAT request replaces the RACSTAT function.

STOKEN. A UTOKEN associated with a user who has submitted work. See *UTOKEN* and *RTOKEN*.

Storage Management Subsystem (SMS). A DFSMS facility used to automate and centralize storage management by providing the storage administrator with control over data class, storage class, management class, storage group, and automatic class selection routine definitions.

structure. See *cache structure*.

stub. (1) A function that connects with the specified library, but remains outside the specified library. (2) A protocol extension procedure.

subject's distinguished name (SDN). The X.509 name in a digital certificate that is associated with the name of the subject.

superuser. In z/OS UNIX, a system user who operates with the special privileges needed to perform a specified administrative task.

superuser authority. In z/OS UNIX, the unrestricted authority to access and modify any part of the operating system, usually associated with the user who manages the system.

supervisor. The part of a control program that coordinates the use of resources and maintains the flow of processing unit operations. Synonym for *supervisory routine*.

supervisor state. A state during which a processing unit can execute input/output and other privileged instructions. Contrast with *problem state*.

supervisory routine. A routine, usually part of an operating system, that controls the execution of other routines and regulates the flow of work in a data processing system. Synonymous with *supervisor*.

syscall. See *callable service*.

sysplex (system complex). Multiple systems communicating and cooperating with each other through multisystem hardware elements and software services to process the installation's workloads.

sysplex communication. An optional RACF function that allows the system to use XCF services and communicate with other systems that are also enabled for sysplex communication.

system authorization facility (SAF). An interface defined by MVS that enables programs to use system authorization services in order to control access to resources, such as data sets and MVS commands. SAF either processes security authorization requests directly or works with RACF, or other security product, to process them.

system call. In z/OS UNIX, a synonym for *callable service*.

system complex. See *sysplex*.

System Management Facility (SMF). The part of the operating system that collects and records system and job-related information used in billing users, reporting reliability, analyzing the configuration, scheduling jobs, summarizing direct access volume activity, evaluating data set activity, profiling system resource use, and maintaining system security. The information is recorded in the SMF log data set.

Systems Network Architecture (SNA). The IBM architecture that defines the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks. The layered structure of SNA allows the ultimate origins and destinations of information, that is, the users, to be independent of and unaffected by the specific SNA network services and facilities used for information exchange.

Glossary

T

tape volume set. The collection of tape volumes on which a multivolume data set resides. A volume set is represented in one RACF profile.

tape volume table of contents (TVTOC). Information about a tape data set that RACF stores in the tape volume profile for the volume on which the data set resides. The TVTOC includes the data set name, data set sequence number, creation date, and an indicator as to whether a discrete tape data set profile exists.

target node. An RRSF node that a given RRSF node is logically connected to, as a result of a TARGET command. See *local node* and *remote node*.

target user ID. The target half of a source user ID and target user ID pair that has an established user ID association between them. For command direction, the target user ID is the user ID specified on the AT or ONLYAT keyword, and is the user ID under whose authority the command is run on the specified node. For password synchronization, the target user ID is the user ID whose password RACF automatically updates when the password for the source user ID is changed. Contrast with *source user ID*.

task. A basic unit of work to be performed or a process and the procedures that run the process.

template. Contains mappings of the profiles on the RACF database.

TOKENBLD request. The issuing of the RACROUTE macro with REQUEST=TOKENBLD specified. A TOKENBLD request builds a UTOKEN.

TOKENMAP request. The issuing of the RACROUTE macro with REQUEST=TOKENMAP specified. A TOKENMAP request maps a token in either internal or external format, allowing a caller to access individual fields within the UTOKEN.

TOKENXTR request. The issuing of the RACROUTE macro with REQUEST=TOKENXTR specified. A TOKENXTR request extracts a UTOKEN from the current address space, task or a caller-specified ACEE.

TP. See *transaction program*.

tranquility. Keeping the security classification of a resource constant while it is in use; keeping the security classification of a user constant while active.

transaction program (TP). A program that processes transactions in an SNA network.

TVTOC. See *tape volume table of contents*.

U

UACC. See *universal access authority*.

UADS. See *user attribute data set*.

universal access authority (UACC). The default access authority that applies to a resource if the user or group is not specifically permitted access to the resource, unless the user is restricted. The universal access authority can be any of the access authorities.

universal group. A user group defined using the UNIVERSAL operand of the ADDGROUP command. Universal groups are expected to have a large number of members and are unlikely to be deleted. Group profiles for universal groups do not contain complete membership information, and the LISTGRP command is not recommended to list members. Using the output of the database unload utility (IRRDBU00) is the best way to list members of a universal group.

user. A person who requires the services of a computing system.

user attribute. The extraordinary privileges, restrictions, and processing environments assigned to a user. The user attributes are SPECIAL, AUDITOR, CLAUTH, OPERATIONS, GRPACC, ADSP, and REVOKE.

user attribute data set (UADS). In TSO, a partitioned data set with a member for each authorized user. Each member contains the appropriate passwords, user identifications, account numbers, LOGON procedure names, and user characteristics that define the user.

user certificate. A type of certificate managed by RACF. See *digital certificate*.

user data set. A data set defined to RACF in which either the high-level qualifier of the data set name or the qualifier supplied by an installation exit routine is a RACF user ID.

user ID. A RACF user ID. A string of 1–8 alphanumeric characters that uniquely identifies a RACF user, procedure, or batch job to the system. For TSO users, the user ID cannot exceed 7 characters and must begin with an alphabetic, #, \$, or @ character. The user ID is defined by a user profile in the RACF database and is used as the name of the profile.

user ID association. A relationship between two user IDs, established through the RACLINK command, which is required for command direction and password synchronization between the user IDs. See *peer user ID association* and *managed user ID association*.

user identification. See *user ID*.

user identification and verification. The acts of identifying and verifying a RACF-defined user to the

system during logon or batch job processing. RACF identifies the user by the user ID and verifies the user by the password, PassTicket, verified digital certificate, DCE credentials, or operator identification card supplied during logon processing or the password supplied on a batch JOB statement.

user identifier (UID). A number between 0 and 2 147 483 647 that identifies a user to z/OS UNIX. The UID is associated with a RACF user ID when it is specified in the OMVS segment of the user profile. It can be contained in an object of type `uid_t`, that is used to identify a system user. When the identity of the user is associated with a process, a UID value is referred to as a real UID, an effective UID, or an (optional) saved set UID. See *real UID*. Contrast with *effective user identifier (effective UID)*.

user name. In RACF, 1–20 alphanumeric characters that represent a RACF-defined user. Contrast with *user ID*.

user profile. A description of a RACF-defined user that includes the user ID, user name, default group name, password, profile owner, user attributes, and other information. A user profile can include information for subsystems such as TSO and DFP.

UTOKEN. The RACF user security token. A UTOKEN is an encapsulation or representation of the security characteristics of a user. RACF assigns a UTOKEN to each user in the system. See *STOKEN* and *RTOKEN*.

V

verification. See *user identification and verification*.

VERIFY request. The issuing of the RACROUTE macro with `REQUEST=VERIFY` specified. A VERIFY request is used to verify the authority of a user to enter work into the system. The VERIFY request replaces the RACINIT function.

VERIFYX request. The issuing of the RACROUTE macro with `REQUEST=VERIFYX` specified. A VERIFYX request verifies a user and builds a UTOKEN, and handles the propagation of submitter ID.

Virtual Machine (VM). (1) An operating system that appears to be at the exclusive disposal of the particular user, but whose functions are accomplished by sharing the resources of a real data processing system. (2) In VM/ESA, the operating system that represents the virtual processors, virtual storage, virtual devices, and virtual channel subsystem allocated to a single user. A virtual machine also includes any expanded storage dedicated to it.

VM. See *Virtual Machine*.

W

workspace data sets. VSAM data sets used by RACF for queuing requests sent to and received from target nodes in an RRSF environment.

X

X.500. ITU/ISO 9594 standard for an open system directory information tree; includes protocols for access and security.

Z

z/OS. A program licensed by IBM that not only includes and integrates functions previously provided by many IBM software products, including the MVS operating system, but also:

1. Is an open, secure operating system for IBM enterprise servers
2. Complies with industry standards
3. Is based on the new 64-bit z/Architecture
4. Supports technology advances in networking server capability, parallel processing, and object-oriented programming

z/OS UNIX group identifier (GID). See *group identifier (GID)*.

z/OS UNIX System Services (z/OS UNIX). The set of functions provided by the shells, utilities, kernel, file system, debugger, Language Environment, and other elements of the z/OS operating system that allows users to write and run application programs that conform to UNIX standards.

z/OS UNIX user identifier (UID). See *user identifier (UID)*.

Glossary

Index

A

ACCESS
 event qualifiers 123
 record extension 121
access control list
 event qualifiers 237, 239
 record extension format 236, 238
access rights
 event qualifiers 225
 record extension 223
accessibility 441
ACEE keyword
 on ICHEINTY macro 320
ACTION keyword
 on ICHNCONV macro 17
 on ICHRFRTB macro 20
ACTIONS keyword
 on ICHEINTY macro 322
ADDGROUP
 event qualifiers 133
 record extension 132
ADDSD
 event qualifiers 132
 record extension 131
ADDUSER
 event qualifiers 135
 record extension 134
ADDDVOL
 event qualifiers 125
 record extension 124
administration
 classroom courses xiii
algorithm
 input data 297
 PassTicket generator 294
 secured signon session key generator 303
ALTDSD
 event qualifiers 136
 record extension 135
ALTGROUP
 event qualifiers 137
 record extension 136
ALTUSER
 event qualifiers 139
 record extension 138
APPC session establishment records 155
APPCLU
 event qualifiers 155
 record extension 154
application key
 description 297

C

CASE keyword
 on ICHERCDE macro 3

CDT (class descriptor table)
 classes supplied by IBM 351
 syntax of the ICHERCDE macro 1, 314
 sysplex communication 2
 when the RACF database is shared 2
CHAIN keyword
 on ICHEINTY macro 321
change audit
 event qualifiers 165
 record extension 162
change directory
 event qualifiers 166
 record extension 165
change file mode
 event qualifiers 169
 record extension 166
change file ownership
 event qualifiers 171
 record extension 169
check directory access
 event qualifiers 160
 record extension 158
check file access
 event qualifiers 162
 record extension format 160
check file owner
 event qualifiers 209
 record extension 207
check privilege
 event qualifiers 210
 record extension 209
CKOWN2
 event qualifiers 223
 record extension 222
class descriptor table (CDT)
 sysplex communication 2
 when the RACF database is shared 2
CLASS keyword
 on ICHEINTY macro 319
 on ICHERCDE macro 3
 on ICHRFRTB macro 20
classroom courses, RACF xiii
clear SETID bits
 event qualifiers 173
 record extension 171
combination field definitions
 definition 393
 format 393
COND keyword
 on ICHETEST macro 330
 on ICHNCONV SELECT macro 11
CONNECT
 event qualifiers 140
 record extension 139
connect template
 contents 407
conversion rules for database unload 258
courses about RACF xiii

customization macros 1

D

data set
 record formats 275
data set template
 contents 409
data unload utility 113
database profile
 storage requirements 393, 395
database unload utility (IRRDBU00) 249
 conversion rules 258
 record formats produced 258
DATAMAP keyword
 on ICHEINTY macro 322
date conversion routine 33
DATEFMT keyword
 on ICHEINTY macro 325
DEFINE
 event qualifiers 130
 record extension 129
DEFINE keyword
 on ICHNCONV macro 10
DELDSD
 event qualifiers 141
 record extension 140
DELGROUP
 event qualifiers 142
 record extension 142
DELRES
 event qualifiers 128
 record extension 127
DELUSER
 event qualifiers 144
 record extension 143
DELVOL
 event qualifiers 129
 record extension 128
DFTRETC keyword
 on ICHERCDE macro 3
DFTUACC keyword
 on ICHERCDE macro 3
directory search
 event qualifiers 158
directory search record extension format 156
disability 441
documents, licensed xiv

E

ENCRYPT keyword
 on ICHEACTN macro 334
 on ICHETEST macro 330
END keyword
 on ICHNCONV macro 18
ENTRY keyword
 on ICHEINTY macro 319
event codes
 for SMF data unload utility 115
 for type 80 SMF records 42

event codes (*continued*)
 qualifier descriptions 421
 qualifiers
 for type 80 SMF records 42
event qualifiers
 ACCESS 123
 access control list 237, 239
 access rights 225
 ADDGROUP 133
 ADDSD 132
 ADDUSER 135
 ADDDVOL 125
 ALTDSD 136
 ALTRGROUP 137
 ALTUSER 139
 APPCLU 155
 change audit 165
 change directory 166
 change file mode 169
 change file ownership 171
 check directory access 160
 check file access 162
 check file owner 209
 check privilege 210
 CKOWN2 223
 clear SETID bits 173
 CONNECT 140
 DEFINE 130
 DELDSD 141
 DELGROUP 142
 DELRES 128
 DELUSER 144
 DELVOL 129
 directory search 158
 EXEC SETGID 174
 EXEC SETUID 174
 for general event record extension 155
 GETPSENT 175
 initACEE 227
 IPCCHK 215
 IPCCTL 220
 IPCGET 217
 JOBINIT 120
 KILL 180
 LINK 181
 MKDIR 184
 MKNOD 187
 mount file system 189
 Network Authentication Service 227
 open slave TTY 211
 OPENFILE 191
 PASSWORD 145
 PERMIT 146
 PTRACE 193
 RACDCERT 226
 RACLINK command 214
 RALTER 147
 RDEFINE 149
 RDELETE 150
 REMOVE 151
 rename file 195

- event qualifiers (*continued*)
 - RENAMEDS 126
 - RMDIR 196
 - RPKIEXPT 230
 - RPKIGENC 229
 - RPKIREAD 233
 - RPKIUPDC 235
 - RPKIUPDR 234
 - RVARY 154
 - SETEGID 198
 - SETEUID 199
 - SETGID 201
 - SETGROUP 222
 - SETROPTS 152
 - SETUID 202
 - SYMLINK 204
 - UNLINK 205
 - unmount file system 207
 - z/OS UNIX 177, 178
- event qualifiers for general events 156
- EVENT variable
 - on ICHNCONV SELECT macro 14
- EXEC SETGID
 - event qualifiers 174
 - record extension 173
- EXEC SETUID
 - event qualifiers 174
 - record extension 173
- extended=length relocate section
 - variable data for type 80 SMF records 60

F

- FIELD keyword
 - on ICHEACTN macro 332
 - on ICHECTEST macro 330
- fields
 - character 393
 - date 392
 - integer 393
 - time 393
- FINAL keyword
 - on ICHNCONV macro 18
- FIRST keyword
 - on ICHERCDE macro 3
- FLDATA keyword
 - on ICHEACTN macro 333
 - on ICHECTEST macro 330
- FLDEF keyword
 - on ICHEINTY macro 324

G

- G variable
 - on ICHNCONV SELECT macro 12
- general resource
 - fields in the profile 413
 - record formats 279
- general template
 - contents 413
- generator algorithm for PassTickets 294

- generator algorithm for secured signon session
 - key 303
- GENERIC keyword
 - on ICHEINTY macro 324
- GENLIST keyword
 - on ICHERCDE macro 4
- GETPSENT
 - event qualifiers 175
 - record extension 174
- GQ variable
 - on ICHNCONV SELECT macro 12
- group
 - maximum number of users in 394
 - record formats 259
 - template for database 395
- GROUP keyword
 - on ICHERCDE macro 4
- group profile
 - description of the fields 396
- group template
 - contents 396

H

- header
 - for SMF records 35

I

- ICH408I message 36
- ICHEACTN macro
 - description 332
 - examples of 343
 - format of DATAMAP=OLD user work area 340
 - format of the user work area DATAMAP=NEW 336, 340
 - syntax 332
 - using it to alter data 339, 342
 - using it to retrieve data when DATAMAP=OLD 340
 - using it to retrieve data with DATAMAP=NEW 336
- ICHEINTY macro
 - description 314
 - examples of 343
 - return codes 326
 - syntax 314
- ICHERCDE macro
 - class descriptor table supplied by IBM 351
 - description 1
 - syntax 2
- ICHECTEST macro
 - considerations when using 331
 - description 329
 - examples of 343
 - syntax 329
- ICHNCONV ACTION macro
 - description 17
 - syntax 17
- ICHNCONV DEFINE macro
 - description 10
 - syntax 10

ICHNCONV END macro
 description 18
 syntax 18
 ICHNCONV FINAL macro
 description 18
 syntax 18
 ICHNCONV macro
 description 9
 example of coding 19
 ICHNCONV SELECT macro
 description 10
 syntax 10
 ICHRFRTB module
 syntax of the ICHRFRTB macro 20
 ICHRFRTB macro
 description 20
 syntax 20
 ICHRRCDX table 351
 ID keyword
 on ICHERCDE macro 4
 initACEE
 event qualifiers 227
 record extension 226
 initialization record (type 81) 96
 initialize z/OS UNIX
 record extension 176
 IPCCHK
 event qualifiers 215
 record extension 214
 IPCCTL
 event qualifiers 220
 record extension 218
 IPCGET
 event qualifiers 217
 record extension 216
 IRRADU00
 record format 113
 IRRDBU00 utility
 record types 249
 IRRDCR00 module 33
 IRRPNL00 module 29

J

JOBINIT
 event qualifiers 120
 record extension 119, 120

K

keyboard 441
 KEYQUAL keyword
 on ICHERCDE macro 4
 KILL
 event qualifiers 180
 record extension 178

L

licensed documents xiv
 LINK
 event qualifiers 181
 record extension 180

M

macros
 that are part of RACF 1
 maximum number of users in group 394
 MAXLENX keyword
 on ICHERCDE macro 4
 MAXLNTH keyword
 on ICHERCDE macro 5
 MEMBER keyword
 on ICHERCDE macro 5
 messages
 ICH408I 36
 MF keyword
 on ICHEACTN macro 334
 on ICHEINTY macro 325
 on ICHETEST macro 331
 MKDIR
 event qualifiers 184
 record extension 182
 MKNOD
 event qualifiers 187
 record extension 184
 mount file system
 event qualifiers 189
 record extension 187

N

NAME keyword
 on ICHNCONV DEFINE macro 10
 NAMETYPE variable
 on ICHNCONV SELECT macro 14
 naming convention 10
 naming convention table
 example of coding 19
 syntax of the ICHNCONV macro 9
 Network Authentication Service
 event qualifiers 227
 record extension 227
 NEWNAME keyword
 on ICHEINTY macro 323
 NEWNAMX keyword
 on ICHEINTY macro 323
 NEXT keyword
 on ICHNCONV END macro 18
 notices 443

O

OLDVOL variable
 on ICHNCONV SELECT macro 15
 open slave TTY
 event qualifiers 211

- open slave TTY (*continued*)
 - record extension 210
- OPENFILE
 - event qualifiers 191
 - record extension 189
- OPER keyword
 - on ICHERCDE macro 5
- operand on COND keyword
 - on ICHNCONV SELECT macro 16
- operation value
 - on ICHEINTY macro 314
- operator on COND keyword
 - on ICHNCONV SELECT macro 16
- OPTIONS keyword
 - on ICHEINTY macro 324
- OTHER keyword
 - on ICHERCDE macro 5

P

- panel driver interface 25
- PassTicket 293
 - definition 293
 - generating 293
 - generator algorithm
 - description of 294
 - secured signon session key generator algorithm
 - description of 303
- password
 - PassTicket as an alternative for 293
- PASSWORD
 - event qualifiers 145
 - record extension 144
- PERMIT
 - event qualifiers 146
 - record extension 145
- Policy Director
 - record extension 231
- POSIT keyword
 - on ICHERCDE macro 6
- processing record 35
- processing record for auditing data sets 100
- product macros 1
- PROFDEF keyword
 - on ICHERCDE macro 8
- profile
 - contents of a data set profile 409
 - contents of a general resource profile 413
 - contents of a group profile 396
 - contents of a user profile 397
 - in database 392
 - locating/updating with ICHEINTY 314
 - repeat groups 392
 - retrieving/altering data with ICHEACTN 332
 - testing for conditions with ICHETEST 329
 - updating on the RACF database with macros 313
- profile name
 - PTKTDATA class 297
- profile name list service routine 29
- PTKTDATA
 - class profile name 297

- PTRACE
 - event qualifiers 193
 - record extension 192
- publications
 - on CD-ROM xii, xiii
 - softcopy xii, xiii

Q

- QCT variable
 - on ICHNCONV SELECT macro 14
- QUAL variable
 - on ICHNCONV SELECT macro 13

R

- RACDCERT
 - event qualifiers 226
 - record extension 225
- RACF
 - classroom courses xiii
 - panel driver interface 25
 - publications
 - on CD-ROM xii, xiii
 - softcopy xii, xiii
 - SMF records 35
- RACF administration
 - classroom courses xiii
- RACF commands
 - SMF command-related data 68
- RACF database
 - connect template 407
 - general template 413
 - group template 396
 - locating/updating a profile with ICHEINTY 314
 - reserved templates 419
 - user template 397
 - using macros to update the profiles 313
- RACF date conversion routine 33
- RACF macros
 - customization macros 1
 - ICHEACTN 313, 332
 - ICHEINTY 313, 314
 - ICHERCDE macro 1
 - ICHETEST 313, 329
 - ICHNCONV 9
 - FINAL 18
 - ICHNCONV macro
 - ACTION 17
 - DEFINE 10
 - END 18
 - SELECT 10
 - ICHRFRTB macro 20
 - internal to RACF 1
 - list of 1
 - product macros 1
- RACF profile name list service routine 29
- RACF report writer
 - types of records it reformats 35
 - where documented xi

RACF router table
 generating entries for 20
 supplied by IBM 21

RACF secured signon PassTicket 293

RACF security topics
 classroom courses xiii

RACGPID on COND keyword
 on ICHNCONV SELECT macro 16

RACGPID3 on COND keyword
 on ICHNCONV SELECT macro 16

RACLINK command
 event qualifiers 214
 record extension 212

RACLIST keyword
 on ICHERCDE macro 8

RACLREQ keyword
 on ICHERCDE macro 8

RACROUTE macro
 relationship to ICHRFRTB macro 20

RACUID on COND keyword
 on ICHNCONV SELECT macro 16

RACUID3 on COND keyword
 on ICHNCONV SELECT macro 16

RACVAR function for REXX execs
 using 349

RALTER
 event qualifiers 147
 record extension 146

RBA keyword
 on ICHEINTY macro 323

RDEFINE
 event qualifiers 149
 record extension 148

RDELETE
 event qualifiers 150
 record extension 149

record dependent section
 of SMF process records 107
 of SMF status records 109

record extension
 ACCESS 121
 access control list 236, 238
 access rights 223
 ADDGROUP 132
 ADDSD 131
 ADDUSER 134
 ADDVOL 124
 ALTDSD 135
 ALTGROUP 136
 ALTUSER 138
 APPCLU 154
 change audit 162
 change directory 165
 change file mode 166
 change file ownership 169
 check file access 160
 check file owner 207
 check privilege 209
 CKOWN2 222
 clear SETID bits 171
 CONNECT 139

record extension (*continued*)
 DEFINE 129
 DELDSD 140
 DELGROUP 142
 DELRES 127
 DELUSER 143
 DELVOL 128
 EXEC SETGID 173
 EXEC SETUID 173
 GETPSENT 174
 initACEE 226
 initialize z/OS UNIX 176
 IPCCHK 214
 IPCCTL 218
 IPCGET 216
 JOBINIT 119, 120
 KILL 178
 LINK 180
 MKDIR 182
 MKNOD 184
 mount file system 187
 Network Authentication Service 227
 OPENFILE 189
 PASSWORD 144
 PERMIT 145
 Policy Director 231
 PTRACE 192
 RACDCERT 225
 RALTER 146
 RDEFINE 148
 RDELETE 149
 REMOVE 150
 rename file 193
 RENAMEDS 125
 RMDIR 195
 RPKIEXPT 229
 RPKIGENC 228
 RPKIREAD 231
 RPKIUPDC 234
 RPKIUPDR 233
 RVARY 153
 SETGID 197, 199
 SETGROUP 220
 SETROPTS 151
 SETUID 198, 201
 SYMLINK 202
 UNLINK 204
 unmount file system 206

record formats
 data set 275, 279
 for database unload utility 258
 group 259
 user 261

records
 SMF 35
 reformatted process 104
 reformatted status 109
 type 80 35
 type 81 96
 type 83 100

- reformatted process records
 - format of 104
 - record dependent section 107
- reformatted SMF records
 - description 104
 - types of 35
- reformatted status records
 - format of 109
 - record dependent section 109
- RELEASE keyword
 - on ICHEACTN macro 335
 - on ICHEINTY macro 320, 331
 - on ICHETEST macro 331
- relocate section
 - for reformatted process records 107
 - for reformatted status records 112
 - variable data for type 80 SMF records 54
- REMOVE
 - event qualifiers 151
 - record extension 150
- rename file
 - event qualifiers 195
 - record extension 193
- RENAMEDS
 - event qualifiers 126
 - record extension 125
- repeat groups
 - in database 392
 - when using ICHETEST macro 331
- report writer
 - types of records it reformats 35
 - where documented xi
- REQSTOR keyword
 - on ICHRFRTB macro 20
- resource class descriptor table 1
- return codes
 - from ICHEINTY macro 326
- REXX RACVAR function
 - using 349
- RMDIR
 - event qualifiers 196
 - record extension 195
- router table
 - generating entries for 20
 - supplied by IBM 21
- RPKIEXPT
 - event qualifiers 230
 - record extension 229
- RPKIGENC
 - event qualifiers 229
 - record extension 228
- RPKIREAD
 - event qualifiers 233
 - record extension 231
- RPKIUPDC
 - event qualifiers 235
 - record extension 234
- RPKIUPDR
 - event qualifiers 234
 - record extension 233

- RUN keyword
 - on ICHEACTN macro 334
 - on ICHEINTY macro 320
- RVARY
 - event qualifiers 154
 - record extension 153
- RVRSMAC keyword
 - on ICHERCDE macro 8

S

- secured signon PassTicket 293
 - generating a session key with 301
- security topics for RACF
 - classroom courses xiii
- SEGMENT keyword
 - on ICHEINTY macro 322
- SELECT keyword
 - on ICHNCONV macro 10
- SET keyword
 - on ICHNCONV ACTION macro 17
- SETEGID
 - event qualifiers 198
- SETEUID
 - event qualifiers 199
- SETGID
 - event qualifiers 201
 - record extension 197, 199
- SETGROUP
 - event qualifiers 222
 - record extension 220
- SETROPTS
 - event qualifiers 152
 - record extension 151
- SETUID
 - event qualifiers 202
 - record extension 198, 201
- shared RACF database
 - caution for class descriptor tables 2
- shortcut keys 441
- SLBLREQ keyword
 - on ICHERCDE macro 9
- SMC keyword
 - on ICHEINTY macro 324
- SMF records
 - description of the types RACF produces 35
 - header portion format 113
 - reformatted 104
 - process records 104
 - status records 109
 - type 80 35
 - type 81 35, 96
 - type 83 35, 100
- SMF80DTP field
 - table of data types 54
- SMF80EVQ field
 - event code qualifier descriptions 421
 - table of event code qualifiers 42
- SMF80EVT field
 - event code qualifier descriptions 421
 - table of event codes 42

- SMF80TP2 field
 - table of data types 60
- storage requirement
 - database profiles 393, 395
- SUBSYS keyword
 - on ICHRFRTB macro 21
- SYMLINK
 - event qualifiers 204
 - record extension 202

T

- Table 1 (event codes and qualifiers)
 - for type 80 SMF records 42
- Table 2 (relocate section variable data)
 - for type 80 SMF records 54
- Table 3 (extended-length relocate section variable data)
 - for type 80 SMF records 60
- Table 4 (command-related data)
 - for type 80 SMF records 68
- templates
 - connect 407
 - data set 409
 - general 413
 - group 396
 - reserved 419
 - user 397
- templates for database
 - combination field definitions 393
 - format of field definitions 391
 - repeat groups 392
- TESTS keyword
 - on ICHEACTN macro 334
 - on ICHEINTY macro 323
- translation table 300
- type 20 SMF record
 - reformatted process records 104
 - when written 104
- type 30 SMF record
 - reformatted process records 104
 - when written 104
- type 80 SMF record
 - description 35
 - events written for 35
 - format of 37
 - list of information contained in 37
 - reformatted process records 104
 - reformatted status records 109
 - table of command- related data 68
 - table of event codes and event code qualifiers 42
 - table of extended-length relocate section variable data 60
 - table of relocate section variable data 54
 - uses for 37
- type 81 SMF record
 - class data format 245
 - description 96
 - events written for 96
 - format of 96
 - reformatted status records 109
 - unloaded data format 241

- type 83 SMF record
 - description 100
 - events written for 100
 - unloaded data format 247
- TYPE keyword
 - on ICHEINTY macro 319
- TYPE=END
 - on ICHRFRTB macro 21

U

- U variable
 - on ICHNCONV SELECT macro 12
- UNLINK
 - event qualifiers 205
 - record extension 204
- unloaded database records 250
- unmount file system
 - event qualifiers 207
 - record extension 206
- UQ variable
 - on ICHNCONV SELECT macro 12
- user
 - record formats 261
- user profile
 - description of the fields 397
- user template
 - contents 397
- users
 - maximum number in group 394

V

- V variable
 - on ICHNCONV SELECT macro 15
- variable on COND keyword
 - on ICHNCONV SELECT macro 11
 - example of initial variable settings 12
- variable on SET keyword
 - on ICHNCONV ACTION macro 17
- VCT variable
 - on ICHNCONV SELECT macro 15
- VOLUME keyword
 - on ICHEINTY macro 322
- VOLUME variable
 - on ICHNCONV SELECT macro 15

W

- WKA, WKB, and WKC variables
 - on ICHNCONV SELECT macro 16
- WKAREA keyword
 - on ICHEINTY macro 323
- WKSP keyword
 - on ICHEINTY macro 320
- WKX, WKY, and WKZ variables
 - on ICHNCONV SELECT macro 16

Y

YES keyword
on ICHEACTN macro 334

Z

z/OS UNIX
event qualifiers 177, 178
process completion record format 177

Readers' Comments — We'd Like to Hear from You

**z/OS
Security Server RACF
Macros and Interfaces**

Publication No. SA22-7682-03

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	<input type="checkbox"/>				

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	<input type="checkbox"/>				
Complete	<input type="checkbox"/>				
Easy to find	<input type="checkbox"/>				
Easy to understand	<input type="checkbox"/>				
Well organized	<input type="checkbox"/>				
Applicable to your tasks	<input type="checkbox"/>				

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? Yes No

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

Name

Address

Company or Organization

Phone No.



Fold and Tape

Please do not staple

Fold and Tape



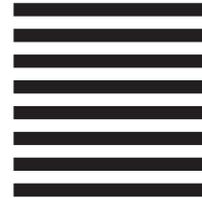
NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

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

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Department 55JA, Mail Station P384
2455 South Road
Poughkeepsie, NY
12601-5400



Fold and Tape

Please do not staple

Fold and Tape



Program Number: 5694-A01, 5655-G52

Printed in U.S.A.

SA22-7682-03

