Security Server RACF
Messages and Codes
This edition applies to version 1, release 13, modification 0 of IBM z/OS (product number 5694-A01) and to all subsequent releases and modifications until otherwise indicated in new editions.
This edition replaces SA22-7686-15.

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

Tables

About this document

Intended audience

How to use this document

Where to find more information

Softcopy documents

RACF courses

To request copies of IBM publications

Using LookAt to look up message explanations

IBM systems center publications

Other sources of information

The z/OS Basic Skills Information Center

How to send your comments to IBM

If you have a technical problem

Summary of changes

Changes made in z/OS Version 1 Release 13

Changes made in z/OS Version 1 Release 12

Changes made in z/OS Version 1 Release 11

Chapter 1. ICH Messages for the system operator

Routing and descriptor codes

Descriptor code descriptions

Routing code descriptions

SAF initialization operator messages

RACROUTE REQUEST=VERIFY operator messages

RACF processing messages

RACF initialization messages

RACF status messages

RACROUTE REQUEST=AUTH operator messages

RACROUTE REQUEST=DEFINE operator messages

Chapter 2. ICH messages for RACF commands

ADDCMD command messages

ADDUSER command messages

CONNECT command messages

REMOVE command messages

DELUER command messages

DELGROUP command messages

PERMIT command messages

PASSWORD command messages

ADDSD and DELDSD command messages

DEFINE command messages

RALTER command messages

DELETE command messages

RLIST command messages

SETOPTS command messages

VARY command messages

ALTGROUP command messages

ALTUSER command messages

ALTDSDF command messages

LISTUSER command messages

SEARCH command messages

LISTGRP command messages

LISTDSD command messages

Chapter 3. Miscellaneous RACF ICH messages

RACF manager error messages

RACF report writer (RACFRW) messages

Data security monitor (DSMON) messages

RACF miscellaneous messages

Chapter 4. IRR messages for RACF database initialization

Routing and descriptor codes

Descriptor code descriptions

Routing code descriptions

VERIFY and VERIFYX messages

RACF processing messages

IRRDPI00 command messages

RACROUTE REQUEST=AUTH VLF messages

RACROUTE REQUEST=VERIFY NJE messages

RACROUTE REQUEST=DEFINE VLF messages

RACROUTE REQUEST=VERIFY NJE messages (Part 2)

VLF cache messages

IBM DB2 external security module for RACF

Chapter 5. IRR messages for the system operator

Routing and descriptor codes

Descriptor code descriptions

Routing code descriptions

VERIFY and VERIFYX messages

RACF processing messages

IRRDPI00 command messages

RACROUTE REQUEST=AUTH VLF messages

RACROUTE REQUEST=VERIFY NJE messages

(RPart 1)

RACF user ID and group ID mapping messages

Dynamic started task messages

RACROUTE REQUEST=VERIFY NJE messages

(RPart 2)

VLF cache messages

IBM DB2 external security module for RACF

Chapter 6. IRR messages for commands, utilities, and other tasks

Messages common to several commands

Dynamic parse (IRRDPL00) messages

RACF cross-reference utility (IRRUT100) messages

RACF database verification (IRRUT200) messages

RACF block update command (BLKUPD) messages

RACF database split/merge utility (IRRUT400) messages

Internal reorganization of aliases utility (IRRIRA00) messages

RACF database unload utility (IRRDBU00) and RACF SMF data unload utility (IRRADU00)

messages

RACF remove ID utility (IRRRID00) messages

REXX RACVAR messages

RACF subsystem messages

DISPLAY command messages

© Copyright IBM Corp. 1994, 2012
## Tables

| 1. | TCP protocol task-name values | 336 |
| 2. | Return codes for the RACF cross-reference utility (IRRUT100) | 409 |
| 3. | Return codes for the database verification utility (IRRUT200) | 410 |
| 4. | Return codes for the RACF database split/merge utility (IRRUT400) | 410 |
| 5. | Return codes for the RACF database unload utility (IRRDBU00) | 411 |
| 6. | Return codes for the SMF data unload utility (IRRADU00) | 412 |
| 7. | Return codes for the internal reorganization of alias utility (IRRIRA00) | 412 |
| 8. | Return codes for the remove ID utility (IRRRI00) | 413 |
About this document

This document supports z/OS® (5694-A01) and contains information about Resource Access Control Facility (RACF®), which is part of z/OS Security Server.

This document includes the messages, abend codes, RACF manager return codes, and RACF utility return codes produced by the Resource Access Control Facility (RACF) component.

If you need explanations of return codes from RACF macros, see z/OS Security Server RACROUTE Macro Reference.

Intended audience

This document is intended for anyone who uses Security Server RACF and wants to know what caused a message to be displayed and what corrective action, if any, needs to be taken.

How to use this document

The messages and codes in this document have been organized into chapters so that the documentation can be separated for easy use (if desired) according to the needs of the installation.

Messages are generally arranged in alphanumeric order by message identifier.

Most RACF messages have message identifiers. If you receive a message without a message identifier, your system may be suppressing the display of message numbers. Enter the following command and re-create the condition that caused the message to be displayed: PROFILE WTPMSG MSGID

If you have a message identifier, you might find the index helpful in finding the message itself.

In this document:

• Chapter 1, “ICH Messages for the system operator,” on page 1 lists and explains the system operator messages that RACF routes to a system console or a security console.
• Chapter 2, “ICH messages for RACF commands,” on page 65 lists and explains messages prefixed by ICH that are issued by RACF commands.
• Chapter 3, “Miscellaneous RACF ICH messages,” on page 149 lists and explains miscellaneous messages prefixed by ICH.
• Chapter 4, “IRR messages for RACF database initialization,” on page 161 lists and explains messages prefixed by IRR that are issued during RACF database initialization.
• Chapter 5, “IRR messages for the system operator,” on page 167 lists and explains messages prefixed by IRR that can go to the system operator.
• Chapter 6, “IRR messages for commands, utilities, and other tasks,” on page 185 lists and explains messages prefixed by IRR that are issued by RACF commands, utilities, and other tasks.
Chapter 7, “IRR messages for callable services,” on page 365 lists and explains messages prefixed by IRR that are issued by the RACF callable services.

Chapter 8, “IBM health checker for z/OS and sysplex messages,” on page 369 lists and explains messages prefixed by IRRH that are issued by RACF to manage the RACF Health Checks.

Chapter 9, “SAF user mapping plug-in related messages,” on page 385 lists and explains messages prefixed by IRRPI that are issued from the SAF plug-in and returned to the calling application.

Chapter 10, “IKJ messages,” on page 391 briefly introduces the TSO messages, and provides a link to z/OS TSO/E Messages where these messages are listed and explained in detail.

Chapter 11, “RACF abend codes,” on page 393 lists and explains the RACF-related abend codes that the system issues to indicate the abnormal completion of a task. Completion codes appear in hexadecimal.

Chapter 12, “RACF return codes,” on page 405 lists and explains the return codes from RACF manager and RACF utilities.

An index is provided to help find messages.

Where to find more information

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

Softcopy documents

The RACF library is available on the following DVD softcopy collection in both BookManager® and Portable Document Format (PDF) files. The collection includes Softcopy Reader, which is a program that enables you to view the BookManager files. You can view or print the PDF files with an Adobe Reader.

SK3T-4271  z/OS Version 1 Release 13 and Software Products DVD Collection

This collection contains the documents for z/OS Version 1 Release 13 and the libraries for multiple releases of more than 400 z/OS-related software products, on DVDs.

The following CD softcopy collection includes books related to RACF:

SK3T-7876  IBM System z Redbooks Collection

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

RACF courses

The following RACF classroom courses are available in the United States:

H3917  Basics of z/OS RACF Administration
H3927  Effective RACF Administration
ES885  Exploiting the Advanced Features of RACF
ES840  Implementing RACF Security for CICS
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)

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 8:30 a.m. through 5:00 p.m. Eastern Time. You can use this number to:

- Order or inquire about IBM publications
- Resolve any software manufacturing or delivery concerns
- Activate the program reorder form to provide faster and more convenient ordering of software updates

Using LookAt to look up message explanations

LookAt is an online facility that lets you look up explanations for most of the IBM 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.

You can use LookAt from these locations to find IBM message explanations for z/OS elements and features, z/VM®, z/VSE, and Clusters for AIX® and Linux:

- Your z/OS TSO/E host system. You can install code on your z/OS systems to access IBM message explanations using LookAt from a TSO/E command line (for example: TSO/E prompt, ISPF, or z/OS UNIX System Services).
- Your Microsoft Windows workstation. You can install LookAt directly from the z/OS and Software Products DVD Collection (SK3T-4271) and use it from the resulting Windows graphical user interface (GUI). The command prompt (also known as the DOS > command line) version can still be used from the directory in which you install the Windows version of LookAt.
- Your wireless handheld device. You can use the LookAt Mobile Edition from [www.ibm.com/servers/eserver/zseries/zos/bkserv/lookat/lookatm.html](http://www.ibm.com/servers/eserver/zseries/zos/bkserv/lookat/lookatm.html) with a handheld device that has wireless access and an Internet browser.

You can obtain code to install LookAt on your host system or Microsoft Windows workstation from:

- The z/OS and Software Products DVD Collection (SK3T-4271).
- The LookAt Web site (click **Download** and then select the platform, release, collection, and location that suit your needs). More information is available in the LOOKAT.ME files available during the download process.
IBM systems center publications

IBM systems centers produce documents known as IBM Redbooks® 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.

GG24-4282  Secured Single Signon in a Client/Server Environment
GG24-4453  Enhanced Auditing Using the RACF SMF Data Unload Utility
GG26-2005  RACF Support for Open Systems Technical Presentation Guide
SG24-4820  OS/390 Security Server Audit Tool and Report Application
SG24-5158  Ready for e-business: OS/390 Security Server Enhancements
SG24-6840  Communications Server for z/OS V1R2 TCP/IP Implementation Guide Volume 7: Security

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.

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:

• Redbooks
  The documents known as IBM Redbooks that are produced by the International Technical Support Organization (ITSO) are available at the following address:

• 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:

• RACF home page
  You can visit the RACF home page on the World Wide Web using this address:

• 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
  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 “Resources” file tab, then select “Downloads” from the list, or go to
http://www-03.ibm.com/systems/z/os/zos/features/racf/goodies.html
The code is also available from 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 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
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.

The z/OS Basic Skills Information Center
The z/OS Basic Skills Information Center is a Web-based information resource
intended to help users learn the basic concepts of z/OS, the operating system that
runs most of the IBM mainframe computers in use today. The Information Center
is designed to introduce a new generation of Information Technology professionals
to basic concepts and help them prepare for a career as a z/OS professional, such
as a z/OS system programmer.
Specifically, the z/OS Basic Skills Information Center is intended to achieve the
following objectives:
• Provide basic education and information about z/OS without charge
• Shorten the time it takes for people to become productive on the mainframe
• Make it easier for new people to learn z/OS.

To access the z/OS Basic Skills Information Center, open your Web browser to the following Web site, which is available to all users (no login required):
http://publib.boulder.ibm.com/infocenter/zos/basics/index.jsp
How to send your comments to IBM

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

Use one of the following methods to send us your comments:
1. Send an email to mhvrdfs@us.ibm.com
3. Mail the comments to the following address:
   IBM Corporation
   Attention: MHVRCFS Reader Comments
   Department H6MA, Building 707
   2455 South Road
   Poughkeepsie, NY 12601-5400
   U.S.A.
4. Fax the comments to us as follows:
   From the United States and Canada: 1+845+432-9405
   From all other countries: Your international access code +1+845+432-9405

Include the following information:
• Your name and address
• Your email address
• Your telephone or fax number
• The publication title and order number:
  z/OS V1R13.0 Security Server RACF Messages and Codes
  SA22-7686-16
• The topic and page number related to your comment
• The text of your comment.

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

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

If you have a technical problem

Do not use the feedback methods listed above. Instead, do one of the following:
• Contact your IBM service representative
• Call IBM technical support
• Visit the IBM support portal at http://www.ibm.com/systems/z/support/
Summary of changes

This document contains terminology, maintenance, and editorial changes to improve consistency and retrievability. Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

Changes made in z/OS Version 1 Release 13

This document contains information that was previously presented in z/OS Security Server RACF Messages and Codes, SA22-7686-15, which supports z/OS Version 1 Release 13.

New information:

The following messages have been added:

- Chapter 8, “IBM health checker for z/OS and sysplex messages,” on page 369: IRRH500I, IRRH501E, IRRH502I, IRRH503E, IRRH504I, IRRH505E, IRRH506I, IRRH507I

Changes made in z/OS Version 1 Release 13

This document contains information that was previously presented in z/OS Security Server RACF Messages and Codes, SA22-7686-14, which supports z/OS Version 1 Release 12.

New information:

The following messages have been added:

- “RACF subsystem messages” on page 248: IRRC040I, IRRC050I, IRRC051I, IRRC052I, IRRC053I, IRRC054I, IRRC055I, IRRC056I, IRRC057I, IRRC058I, IRRC059I, IRRC060I, IRRC061I, IRRC062I, IRRC063I, IRRC064I
- “TARGET command messages” on page 315: IRRM087I, IRRM088I, IRRM089I, IRRM090I, IRRM091I, IRRM092I, IRRM093I, IRRM094I, IRRM095I, IRRM096I, IRRM097I
- “RRSF connection receive transaction program messages” on page 328: IRRN001I, IRRN010I
- “RRSF connection task messages” on page 335: IRRQ001I, IRRQ010I, IRRQ180I, IRRQ181I
- “RACMAP command messages” on page 356: IRRW214I, IRRW215I, IRRW216I

Changed information:

The following messages have been changed:

- “RDELETE command messages” on page 102: ICH12304
- “SETROPTS command messages” on page 105: ICH14078
- Chapter 3, “Miscellaneous RACF ICH messages,” on page 149: ICH66102I
- “RACROUTE REQUEST=AUTH VLF messages” on page 177: IRR803I
Changes made in z/OS Version 1 Release 12

This document contains information that was previously presented in z/OS Security Server RACF Messages and Codes, SA22-7686-13, which supports z/OS Version 1 Release 11.

New information:

The following messages have been added:

- "RDEFINE command messages" on page 92 ICH10321I
- "RDELETE command messages" on page 102 ICH12306I
- Chapter 6, "IRR messages for commands, utilities, and other tasks," on page 185 IRRH083I, IRRH084I
- "RACDCERT command messages" on page 276 IRRD185I, IRRD186I, IRRD187I, IRRD188I, IRRD189I, IRRD197I
- "R_PKIServ callable service messages" on page 365 IRRD210I

Changed information:

The following messages have been changed:

- "RLIST command messages" on page 104 ICH13007I
- "SETROPTS command messages" on page 105 ICH14078
- "RACROUTE REQUEST=AUTH VLF messages" on page 177 IRR803I
- "RACDCERT command messages" on page 276 IRRD108I, IRRD109I, IRRD125I
- "RACDCERT command messages" on page 276 IRRD156I, IRRD171I
- "R_PKIServ callable service messages" on page 365 IRRD207I
- "R_PKIServ callable service messages" on page 365 IRRD203I
- Chapter 8, "IBM health checker for z/OS and sysplex messages," on page 369 IRRH229E
- "File allocation messages" on page 350 IRRU080I
- "RRSF operational modes and coupling facility messages" on page 359 IRRXX004A

The "Readers' Comments - We'd Like to Hear from You" section at the back of this publication has been replaced with "How to send your comments to IBM" on page xiii
Changes made in z/OS Version 1 Release 11

This document contains information that was previously presented in z/OS Security Server RACF Messages and Codes, SA22-7686-12, which supports z/OS Version 1 Release 10.

New information:

The following messages have been added:
- “DELUSER command messages” on page 76: ICH04018I
- “RACF subsystem messages” on page 248: IRRRC132I, IRRRC144I
- “RACDCERT command messages” on page 276: IRRD132I, IRRD130I
- “RACMAP command messages” on page 356: IRRD190I, IRRD191I, IRRD192I, IRRD193I, IRRD194I, IRRD195I, IRRD196I

The following reason codes have been added for the 283 abend code:
- 6C
- 70

The following topics have been added:
- “IRRADU00 return codes” on page 411
- “IRRRI00 return codes” on page 413

Changed information:

The following messages have been changed:
- “RACF processing messages” on page 5: ICH408I
- “RACF initialization messages” on page 33: ICH555I
- “SETROPTS command messages” on page 105: ICH14079I
- “RACF miscellaneous messages” on page 159: ICH70001I
- Chapter 4, “IRR messages for RACF database initialization,” on page 161: ICH8025I
- “RACF processing messages” on page 171: IRR417I
- “RACF database unload utility (IRRDBU00) and RACF SMF data unload utility (IRRADU00) messages” on page 235: IRR67653I
- “RACF subsystem messages” on page 248: IRRRC132I
- “RACDCERT command messages” on page 276: IRRD109I, IRRD130I

“RACF utility return codes” on page 409 has been restructured.

Deleted information:
- The second bullet in the explanation of message ICH70001I in “RACF miscellaneous messages” on page 159 has been removed.
Chapter 1. ICH Messages for the system operator

This chapter lists the system operator messages that the Resource Access Control Facility (RACF) routes to a system console or a security console.

The format of these messages is:
ICH<nn>nt text

where:
ICH identifies the message as a RACF message.
x identifies the RACF function, where:
0 = SAF initialization
3 = RACROUTE REQUEST=VERIFY macro
4 = RACF processing
5 = RACF initialization
7 = RACF status
8 = RACROUTE REQUEST=AUTH macro
9 = RACROUTE REQUEST=DEFINE macro

nn is the message serial number.
t is the type code, where:
A = Action; operator must perform a specific action.
D = Decision; operator must choose an alternative.
E = Eventual action required.
I = Information; no operator action is required.
W = Wait; processing stops until action is determined and performed.
text is the text of the message.

Routing and descriptor codes

The routing and descriptor codes for these messages are shown with the message explanations.

Descriptor code descriptions

Descriptor codes indicate the significance of a message. Specifically, descriptor codes let the user know the status of the system itself or that of a specific task:
Has it stopped processing?
Is it waiting for another action to be completed?
Or, is it continuing to process?

In addition, this code determines how the system will display and delete the message.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>System Failure</td>
</tr>
</tbody>
</table>
The message indicates a catastrophic error. To continue, the operator must re-IPL the system or restart a major subsystem.

2 Immediate Action Required

The message indicates that the operator must perform an action immediately. The message issuer can be in a wait state until the action is performed, or the system needs the action as soon as possible to improve performance. The task waits for the operator to complete the action.

Note: When an authorized program issues a message with descriptor code 2, a DOM macro instruction must be issued to delete the message after the requested action is performed.

4 System Status

The message indicates the status of a system task or of a hardware unit.

6 Job Status

The message indicates the status of a job or job step.

Routing code descriptions

Routing codes send system messages to the consoles where they are to be displayed. To send a message to more than one console, RACF assigns more than one routing code to the message. For more information about message routing, see your MVS routing and descriptor codes documentation.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Master Console Action</td>
</tr>
<tr>
<td></td>
<td>The message indicates a change in the status of the system. It demands action by the master console operator.</td>
</tr>
<tr>
<td>2</td>
<td>Master Console Information</td>
</tr>
<tr>
<td></td>
<td>The message indicates a change in the status of the system. It does not demand action; rather, it alerts the master console operator to a condition that may require action.</td>
</tr>
<tr>
<td></td>
<td>This routing code is used for any message that indicates job status when the status is not requested specifically by an operator inquiry. It is also used for processor and problem program messages to the system operator.</td>
</tr>
<tr>
<td>9</td>
<td>System Security</td>
</tr>
<tr>
<td></td>
<td>The message gives information about security checking, for example, a request for a password.</td>
</tr>
<tr>
<td>11</td>
<td>Programmer Information</td>
</tr>
<tr>
<td></td>
<td>The message is intended for the problem programmer. This routing code is used only when the program issuing the message cannot route the message to the programmer by using the system output (SYSOUT) data set. The message appears in the job log.</td>
</tr>
</tbody>
</table>

Note: Routing code 11 is ignored if specified for a multiple-line WTO macro instruction.

SAF initialization operator messages
ICH001E  SAF IS NOT ACTIVE, SDUMP TAKEN
Explanation:  The system authorization facility (SAF) is not active. This message is preceded by another message that explains why and is followed by message ICH006D.
System action:  The SAF error exit requests a dump and issues message ICH006D.

ICH002I  UNABLE TO OBTAIN STORAGE FOR SAF INITIALIZATION
Explanation:  The system authorization facility (SAF) issued a GETMAIN macro for storage in the system queue area (SQA), which is subpool 265, to build the ICHSAFV control block. The GETMAIN failed.
System action:  The SAF error exit issues message ICH001E.

ICH003I  UNABLE TO LOCATE SAF ROUTER (ICHSFR00) IN LPA
Explanation:  The system cannot locate the system authorization facility (SAF) load module, ICHSFR00, in the link pack area (LPA).
System action:  The SAF error exit issues message ICH001E.

ICH004I  SYSTEM ERROR DURING SAF INITIALIZATION
Explanation:  During initialization of the system authorization facility (SAF), a program check occurred. The SAF error exit was invoked.
System action:  The SAF error exit issues message ICH001E.

ICH005I  ACTIVE SAF EXIT: ICHRTX00
Explanation:  The system authorization facility (SAF) installation exit module, ICHRTX00, is in use.
System action:  System initialization proceeds.

ICH006D  RE-IPL OR REPLY U TO CONTINUE WITHOUT SAF
Explanation:  The system authorization facility (SAF) error exit issues this message after ICH001E to let the operator decide whether to continue without SAF or to re-IPL.
System action:  System initialization stops until the operator replies.
Operator response:  Reply U to continue initialization without SAF. Otherwise, correct the problem and re-IPL the system, so that SAF can be included.
RACROUTE REQUEST=VERIFY operator messages

ICH301I  MAXIMUM PASSWORD ATTEMPTS BY SPECIAL USER userid [AT TERMINAL terminalid.]

Explanation: The user specified by userid has made more than the permissible number of attempts to enter a password or password phrase. If this was not a batch job, the last attempt was from the terminal specified by terminalid. Because the specified user has the SPECIAL attribute, the RACF security administrator has the option of not revoking the user. This message is followed by message ICH302D.

The permissible number of password attempts is set using the command

SETROPTS PASSWORD(REVOKE(number_invalid_passwords)

Destination: Descriptor code is 4. Routing code is 9.

ICH302D  REPLY Y TO ALLOW ANOTHER ATTEMPT OR N TO REVOKE USERID userid.

Explanation: This message, which is preceded by a number, follows message ICH301I.

System action: If the response is Y, the logon attempt by the specified user is allowed to continue. If the response is N, the specified user ID is revoked.

Operator response: Reply with either Y or N.

Destination: Descriptor code is 2. Routing code is 9.

Note: In multiple-user address spaces that have a single signon task (such as CICS or IMS), when the signon task issues the message, no other signons can occur until the operator has replied to the message.

ICH303I  INACTIVE INTERVAL EXCEEDED BY USER userid (AT TERMINAL terminalid).

Explanation: The user specified by userid has not accessed the system and had the last access interval updated within the limit specified by SETROPTS INACTIVE(unused-userid-interval). If this was not a batch job, the last attempt was from the terminal specified by terminalid. Because the specified user has the SPECIAL attribute, the RACF security administrator has the option of not revoking the user. This message is followed by ICH304D.

Destination: Descriptor code is 4. Routing code is 9.

ICH304D  REPLY Y TO ACTIVATE USER OR N TO REVOKE USERID userid.

Explanation: This message, which is preceded by a number, follows message ICH303I.

System action: If the response is Y, the logon attempt by the specified user is allowed to continue. If the response is N, the specified user ID is revoked.

Operator response: Reply with either Y or N.

Destination: Descriptor code is 2. Routing code is 9.

Note: In multiple-user address spaces that have a single signon task (such as CICS or IMS), when the signon task issues the message, no other signons can occur until the operator has replied to the message.
Note on the ICH408I messages
Message ICH408I is a set of messages that are displayed in multiple lines. The first line of an ICH408I message identifies a user or job that had an authorization problem. The other lines of the messages (shown in this document following the explanation of USER or JOB) describe the request the user or job was issuing and the reason for the failure.

See the following example:

ICH408I USER(SMITH ) GROUP(DEPT60 ) NAME(R.L.SMITH )
ICH408I DEPT58.CLIST.CNTL CL(DATASET ) VOL(TSO035)
ICH408I INSUFFICIENT ACCESS AUTHORITY
ICH408I FROM DEPT58.CLIST.* (G)
ICH408I ACCESS INTENT(READ ) ACCESS ALLOWED(NONE )

This message can be interpreted as:

User SMITH, a member of group DEPT60, whose name is R.L.SMITH, had INSUFFICIENT ACCESS AUTHORITY to resource DEPT58.CLIST.CNTL, which is in class DATASET and resides on volume TSO035.

The RACF profile protecting the resource is DEPT58.CLIST.*, and it is a generic profile.

The access attempted by SMITH was READ, and the access allowed by RACF was NONE.

Each set of ICH408I messages contains at least one line that describes the reason for failure, typically in the 2nd or 3rd line. Each line of reason for failure is listed and described in alphabetic order in this RACF Processing Messages section.

<table>
<thead>
<tr>
<th>ICH408I</th>
<th>USER (userid) GROUP (group-name)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NAME (user-name) --or-- JOB (jobname)</td>
</tr>
<tr>
<td></td>
<td>STEP (stepname) [SUBMITTER (userid)]</td>
</tr>
<tr>
<td></td>
<td>[PRIMARY USER (userid)] [resource-name]</td>
</tr>
<tr>
<td></td>
<td>[CL(class-name)] --or-- [VOL(volume-id)]</td>
</tr>
<tr>
<td></td>
<td>[FID(file-identifier)] [ID(IPC-identifier)]</td>
</tr>
<tr>
<td></td>
<td>--or-- [FROM generic-profile-name (G)]</td>
</tr>
<tr>
<td></td>
<td>[ACCESS INTENT(intent) ACCESS ALLOWED(allowed)] [EFFECTIVE UID (nnnnnnnnn)] [EFFECTIVE GID (nnnnnnnnn)]</td>
</tr>
</tbody>
</table>

Explanation: This message is issued when RACF detects an unauthorized request (a violation) made by a user or job. The user and group indicated in the first line of the ICH408I message are the execution user ID and group ID under which the job was to run.

If the message indicates a job and step instead of a user, group, and name, RACF cannot find a valid ACEE containing user, group, and name information. This can occur for a started task that is not defined in the RACF started procedures table (ICHRIN03), if an entry in the started procedures table has an incorrect RACF group specified, or if the user’s ACEE has been corrupted. If the submitting user ID is not the same as the execution user ID, the message includes an additional line containing the submitting user ID, group, and node.

When the message is reporting an access failure for a delegated resource using a nested ACEE, PRIMARY USER is displayed. A nested ACEE is an ACEE for a client which indicates the identity of the server or daemon that created the work unit. The client user ID is displayed as the primary user. The first line of this message identifies the server or daemon on whose behalf the resource is being accessed. You should permit the daemon to the resource rather than the client. See z/OS Security Server RACF Security Administrator’s Guide for information about delegated resources and nested ACEEs. Depending on the resource name, consult the appropriate application documentation for setup requirements.

When USER(userid) contains a userid in the form of...
ICH408I

“**mxxxx”, such as “**01XUSR”, the userid identifies an identity context reference, not a RACF user ID. This value, along with a password substitution value, can be used to retrieve information about an authenticated user from an identity cache. See z/OS Integrated Security Services EIM Guide and Reference for more information about identity cache support. When an identity context reference is specified on a RACROUTE REQUEST=VERIFY,ENVIR=CREATE request, RACF will attempt to resolve the reference to a RACF-defined user from the identity cache. If RACF cannot resolve the reference, any resulting ICH408I messages will contain the unresolved identity context reference user value. Possible reasons that the identity context reference cannot be resolved include:

- An invalid value, such as an unsupported SESSION=type value, was specified with the identity context reference on a RACROUTE REQUEST=VERIFY,ENVIR=CREATE request.
- The identity context reference was not recognized by the identity cache. Possible reasons include:
  - The identity context reference was invalid. A valid identity context reference consists of both an 8-character user ID value and an 8-character password value.
  - The identity context reference was expired. Identity context references have a timeout interval of 1 to 3600 seconds (1 hour).
- The identity cache contains invalid or incomplete information. This can happen if the identity cache is not configured to ensure that an identity context reference always resolves to a RACF-defined user (MAPREQUIRED=NO). See z/OS Integrated Security Services EIM Guide and Reference for more information about how to configure the identity cache.

When the message is reporting an access failure for an z/OS UNIX file, the resource name is the pathname that was specified to the kernel syscall. It will not exist for the syscalls performed against open files (those in the “foXXX” format such as fchown). The FID (file identifier) is a unique 32-hex-digit identifier of the file. It is provided because multiple pathnames can be used to access the same file. This identifier will allow matching of accesses to the same file by different names.

When the message is reporting an access failure for an z/OS UNIX IPC key, the resource name is the IPC key name that was specified to the kernel syscall. It is displayed as a unique 8-hex-digit identifier. The ID (IPC identifier) is a unique decimal identifier of the resource. It is provided as additional information, that may be useful during auditing, although it is dynamically allocated by the kernel. It is a numeric value between 0 and 4294967295.

The meaning of the volume serial number shown in the VOL field varies. For a non-VSAM data set, it means the volume on which the data set resides. For a VSAM data set, it means the volume on which the catalog containing the data set entry resides.

The phrase FROM generic-profile-name (G), if included in the message, identifies the generic profile that RACF used to check for access to the resource.

| Note: If used against a DATASET resource-name, and the data set is on tape, then the FROM generic-profile-name might be a TAPEVOL profile, if the TAPEVOL class is active.

For further explanations of this message, check the message line that indicates what request was made. This is typically line 2 or 3. For example, it can be INSUFFICIENT ACCESS AUTHORITY. Find this message line among the explanations that follow for message ICH408I (arranged alphabetically), and read the explanation for that message line.

For attempts to use protected resources, the message shows the access attempted (ACCESS INTENT phrase) and the access permitted by RACF (ACCESS ALLOWED phrase). When the message is reporting an attempt to access an z/OS UNIX file or IPC key, the ACCESS INTENT (intent) is specified as “RWX”, representing read, write or search/execute permission requested. More than one permission can be requested at a time. If a permission is not requested, the letter is replaced by a dash “-“.

ACCESS ALLOWED (allowed) is specified as “(OWNER/GROUP/OTHER/ACL USER/ACL GROUP/NO/RESTRICTED) RWX”, where OWNER indicates the owner permission bits were used, GROUP indicates the group permission bits were used, OTHER indicates the other permission bits were used, ACL USER indicates that a specific user Access Control List (ACL) entry was used, ACL GROUP indicates a specific group ACL entry (or entries) was used, NO indicates that no permission bits were used, RESTRICTED indicates the OTHER bits were not used for a RESTRICTED user, and “RWX” represents the settings of the permission bits that were checked. ACCESS ALLOWED (NO --X) occurs if a superuser attempts to execute a file that does not have OWNER, GROUP, ACL, or OTHER execute permission. ACCESS ALLOWED (RESTRICTED ———) occurs if a RESTRICTED user can have only gained file access by way of the OTHER bits, but the RESTRICTED.FILESYS.ACCESS profile in the UNIXPRIV class has forbidden this.

Note that while checking for group access, the group permission bits are treated as simply another GID ACL entry, if the process GID, or one of its supplemental GIDs matches the file owner GID. Several group entries may actually be checked, and access will be granted if any of them specifies the requested permissions. However, if none of the entries grants the requested access, there is no single entry that defines the access allowed. By convention, the permissions associated with the first relevant group entry encountered are
what will be displayed in the message. See the z/OS UNIX information in z/OS Security Server RACF Security Administrator's Guide for a description of the algorithm used to determine access when an ACL exists for a file or directory.

For violations occurring in the UNIX System Services environment, the user's effective UID and effective GID are displayed in the message. These ids were used to determine the user's privilege for the intended operation. Note that they may not always match the ids defined in the relevant RACF USER and GROUP profiles, because UNIX System Services provides methods by which another identity can be assumed.

System action: If the phrase RESOURCE NOT PROTECTED appears in the message with a warning, RACF allows the request to continue. If the phrase RESOURCE NOT PROTECTED appears in the message without a warning, RACF fails the request.

Notes:
1. When a user is denied access to a RACF-protected resource because of the return code from a RACROUTE REQUEST=AUTH installation exit routine, the user’s allowed access may be inconsistent with the requested access. (For example, access allowed was ALTER, access requested was READ, but the request for access was denied.)

2. Authority checking for users with the restricted attribute bypasses checking of some authority granting mechanisms, such as the UACC. If a LISTUSER for the user ID shows that the user is restricted, the user's user ID or group name must be on the access list to allow access to the resource. See z/OS Security Server RACF Security Administrator’s Guide for additional information about restricted access user IDs.

3. The phrase “LOGON/JOB INITIATION/initACEE” may appear during logon processing; however, the logon may be successful. When RACF is active, logon verification can produce an error during RACF processing; however, the logon can proceed using an alternate method (for example, UADS). This error occurs if the installation does not use the RACF database to store security-related information for a particular user, but it does use an alternate method (such as UADS) for the logon application (for example, TSO) to perform user verification.

4. If the failure occurred for a z/OS UNIX System Services system function, RACF returns an error return code to the invoking system function, which will return an error return code to the application caller or will cause the calling task to abend. See z/OS UNIX System Services Programming: Assembler Callable Services Reference to determine the action of the syscall functions.

5. If you see JOB/STEP in the message instead of USER/GROUP, it indicates a default security environment for an undefined user has been assigned, instead of a normal userid. This can happen if a started procedure is not defined correctly in the STARTED class or in ICHRIN03.
   - If you used the STARTED class, make sure that you have the correct profile(s) defined and make sure that it was properly RACLIST REFRESHed after you added the profiles.
   - If you used ICHRIN03, be sure to IPL the system with CLPA.

For third-party authorization checking, RACF performs the following steps:
   - If the USERID= keyword is omitted, “*” is the default.
   - If the USERID keyword is *NONE* and GROUPID is not specified, RACF checks using a default (undefined-user) ACEE.
   - If USERID=BLANKS is specified (where BLANKS is eight characters of X’40’ characters) and GROUPID is not specified or specified as GROUPID=BLANKS, RACF will build an ACEE with an asterisk (*) specified as the user ID or group name. This is the same as an ACEE built by RACROUTE REQUEST=VERIFY without specifying USERID, GROUPID, or PASSWORD.

User response: Follow the security procedures established for your installation. If no such procedures have been established, report the complete text of this message to the RACF security administrator.

Operator response: Follow the security procedures established for your installation. If no such procedures have been established, report the complete text of this message to the RACF security administrator.

Problem Determination: Detailed information about the violation is available in the SMF type 80 record that RACF produces at the same time as this message. See z/OS Security Server RACF Auditor’s Guide for information about reporting on the contents of the RACF SMF records.

Notes:
1. When RACF verifies a password during logon or when a batch job begins, the message includes NAME (???) .

2. For users not defined to RACF, the job and step are indicated by jobname and stepname. JOB/STEP is used in the following conditions:
   - When there is no ACEE,
   - When the ACEE is invalid, corrupted, or missing key information, or
   - When the ACEE is a default ACEE (that is, uses the undefined user of “*”).

For batch users, stepname is blank.

Destination: Descriptor code is 4. Routing codes are 9 and 11. This message is routed to the security console. All violations (except LOGON/JOB initiation/initACEE

Chapter 1. ICH Messages for the system operator 7
messages, command violations, and z/OS UNIX System Services violations) are issued as write-to-programmer (WTP) messages.

Note: A TSO/E user who is using z/OS UNIX System Services does not see the ICH408I messages.

ICH408I DEFINE - GROUP NOT DEFINED

Explanation: This error occurs when RACF detects an unauthorized attempt to define a RACF-protected resource; for example, by way of RDEFINE for a general resource or ADDSD for a data set.

System action: RACF prevents the request from completing.

User response: Correct any spelling errors in the group ID and try again. If you cannot remember the correct group ID, ask your RACF security administrator to provide you with a valid group ID.

ICH408I DEFINE - INSUFFICIENT AUTHORITY

Explanation: This error occurs when RACF detects an unauthorized attempt to define a RACF-protected resource; for example, by way of RDEFINE for a general resource or ADDSD for a data set. This message can also be issued for certain types of create and rename requests.

System action: RACF prevents the request from completing.

ICH408I DEFINE - RESOURCE ALREADY DEFINED

Explanation: This error occurs when RACF detects an unauthorized attempt to define a RACF-protected resource; for example, by way of RDEFINE for a general resource or ADDSD for a data set.

System action: RACF prevents the request from completing.

ICH408I DEFINE - RESOURCE NOT PROTECTED

Explanation: This error occurs when RACF detects an unauthorized attempt to define a resource that requires RACF protection, such as an MVS data set when the SETROPTS PROTECTALL option is in effect.

System action: RACF prevents the request from completing.

ICH408I DEFINE - USER IN SECOND QUALIFIER IS NOT RACF-DEFINED

Explanation: This error occurs when RACF detects an unauthorized attempt to define a RACF-protected resource. The user specified a profile name in which the second qualifier was not a RACF-defined user ID.

System action: RACF prevents the request from completing.

User response: Correct the second qualifier in the profile name and try again.

ICH408I DEFINE - USER NOT MEMBER OF GROUP

Explanation: This error occurs when RACF detects an unauthorized attempt to define a group data set and create a discrete profile to protect it. To create a discrete profile for a group data set, CREATE authority in that group is required.

System action: RACF prevents the request from completing.

User response: Either:
- Ensure that you are a member of the group and that you have CREATE authority in that group. Or,
- Do not create a discrete profile for the data set, but allow RACF to use an existing generic profile instead.

ICH408I DEFINE - USER NOT RACF-DEFINED

Explanation: This error occurs when RACF detects an unauthorized attempt to define a RACF-protected resource.

System action: RACF prevents the request from completing.

ICH408I DEFINE - WARNING: INSUFFICIENT SECURITY LABEL AUTHORITY

Explanation: This error occurs when RACF detects an unauthorized attempt to define a resource that has a security label associated with it.

System action: RACF allows the request to complete.

User response: If the security label is misspelled, try again. You might need to log off and log on again with a different security label. For a list of security labels you can specify, enter the following RACF command:

```
SEARCH CLASS(SECLABEL)
```

To find out which security label applies to the task you are currently doing, see your installation security procedures or ask your RACF security administrator.

ICH408I DEFINE - WARNING: RESOURCE NOT PROTECTED

Explanation: This error occurs when RACF detects an unauthorized attempt to define a RACF-protected resource.

System action: RACF allows the request to complete.
ICH408I  DEFINE - WARNING: SECURITY LABEL MISSING FROM USER, JOB, OR PROFILE

Explanation:  RACF issues this message when a security label is missing from one of the following:

- The user profile
- A batch job
- A resource profile necessary for logon or job initiation.

and the SETROPTS MLACTIVE(WARNING) option is in effect.

System action:  RACF allows the request to complete.

User response:  If a line of this message indicates a profile in a RACF class, such as SMITH.CLIST CL(DATASET) VOL(D58000), the indicated resource profile is missing a security label. If a security label is not specified for the profile before the installation puts the SETROPTS MLACTIVE(FAILURES) option into effect, you will not be able to log on or submit the job.

ICH408I  DELETE - INVALID VOLUME

Explanation:  This error occurs when RACF detects an unauthorized attempt to delete a RACF-protected resource.

System action:  RACF prevents the request from completing.

ICH408I  DELETE - RESOURCE NOT FOUND

Explanation:  This error occurs when RACF detects an unauthorized attempt to delete a RACF-protected resource.

System action:  RACF prevents the request from completing.

ICH408I  DIGITAL CERTIFICATE SUPPLIED TO AUTHENTICATE USER userid IS NOT TRUSTED. CERTIFICATE SERIAL NUMBER(serial-number) SUBJECT(subject-name) ISSUER(issuer-name).

Explanation:  A user attempted to access a server using a digital certificate that is not trusted. If the user is supplying the correct certificate, and it should be associated with a RACF user ID, use the RACDCERT command to ADD the certificate for the user, or associate it with a user ID with the MAP function. If a certificate mapping already exists for the certificate and it has additional criteria specified, check for an entry in SYS1.LOGREC to determine if an error was encountered attempting to locate the corresponding DIGTCRIT profile.

ICH408I  DIGITAL CERTIFICATE DEFINED TO A RESERVED USER ID. CERTIFICATE SERIAL NUMBER(serial-number) SUBJECT(subject-name) ISSUER(issuer-name).

Explanation:  A user attempted to access a server using a digital certificate that is defined to one of RACF's reserved user IDs. RACF cannot create a security context (ACEE) for this certificate.

System action:  InitiACEE processing ends.

User response:  Ensure that the user is supplying the correct certificate. If the user is supplying the correct certificate, and it should be associated with a RACF user ID, use the RACDCERT command to move the certificate to the correct user ID, or associate it with a user ID with the MAP function. If a certificate mapping already exists for the certificate and it has additional criteria specified, check for an entry in SYS1.LOGREC to determine if an error was encountered attempting to locate the corresponding DIGTCRIT profile.

ICH408I  DISTRIBUTED IDENTITY IS NOT DEFINED: distributed-identity-information

Explanation:  A user attempted to access a server using a distributed identity that is not associated with a RACF user ID. RACF cannot determine a user ID for this user.

System action:  InitiACEE or RACROUTE processing ends.

User response:  Ensure that the user provides the correct identity information. You can associate the distributed identity information with a RACF user ID using the RACMAP command. If the distributed information is already associated with a RACF user ID you can check the SYS1.LOGREC log to determine...
whether an error was encountered while locating the corresponding IDIDMAP profile.

**ICH408I**

**FULL VIOLATION ON COMMAND**

**Command**

**Explanation:** This error occurs when RACF detects an unauthorized attempt to use a RACF command that would modify profiles on the RACF database.

**System action:** RACF prevents the command from completing.

**ICH408I**

**INCORRECT CERTIFICATE SPECIFIED FOR VERIFICATION**

**Explanation:** A user attempted to verify a digital certificate using the R_PKIServ callable service function VERIFY. The attempt failed because the certificate supplied is not known to PKI Services.

**System action:** R_PKIServ processing ends. The certificate is not eligible for renewal or revocation by PKI Services.

**User response:** Check that you have provided the correct certificate for verification. If using a web browser, close all browser windows and restart browser before trying again.

**ICH408I**

**INCORRECT PASS PHRASE SPECIFIED FOR DIGITAL CERTIFICATE EXPORT**

**Explanation:** A user attempted to retrieve a PKI Services digital certificate using the R_PKIServ callable service function EXPORT, but provided an incorrect Certificate ID/pass phrase combination.

**System action:** R_PKIServ processing ends. RACF prevents the request from completing.

**User response:** Check that you have provided the correct Certificate ID and pass phrase for the certificate you are trying to export.

**ICH408I**

**INCORRECT TRANSACTION ID SPECIFIED FOR SCEP DIGITAL CERTIFICATE REQUEST**

**Explanation:** A user attempted to use the R_PKIServ callable service function, SCEPReq, to request a certificate using the Simple Certificate Enrollment Protocol (SCEP), but the input transaction id for the GetCertInitial request is incorrect.

**System action:** R_PKIServ processing ends. RACF prevents the request from completing.

**User response:** See your security administrator.

**RACF Security Administrator Response:** Make sure the transaction ID for the GetCertInitial request is the same as the original PKCSReq request.

**ICH408I**

**INITACEE - USER SECURITY LABEL NOT COMPATIBLE WITH SERVER**

**Explanation:** Different security labels are associated with the user task and the server address space and they are not equivalent.

**System action:** InitACEE processing fails.

**User response:** Ensure that you are using the correct security label for your session, and that you are accessing the correct server.

**ICH408I**

**INSUFFICIENT ACCESS AUTHORITY**

**Explanation:** This error occurs when RACF detects an unauthorized attempt to access a RACF-protected resource.

**System action:** RACF denies the requested access.

**ICH408I**

**INSUFFICIENT AUTHORITY TO EXTEND TO A NEW VOLUME**

**Explanation:** This error occurs when RACF detects an attempt to specify an unauthorized volume on the ADDVOL or CHGVOL operand.

**System action:** RACF denies the request.

**ICH408I**

**INSUFFICIENT AUTHORITY TO syscall-name [CMD(subcommand)]: UNABLE TO PROCESS ACL [SECURITY LABEL FAILURE]**

**Explanation:** This error occurs when RACF detects an attempt to specify an z/OS UNIX function for which the user does not have authority. Syscall-name identifies the z/OS UNIX callable service that invoked RACF. Subcommand identifies the subcommand of syscall-name, where appropriate. If present, subcommand is either IPC_RMID or IPC_SET. The text "UNABLE TO PROCESS ACL" will be displayed if a file access check detected that an ACL exists for the file, but it cannot be retrieved. In this case, the "ACCESS INTENT ...ACCESS ALLOWED..." portion of ICH408I will not be displayed. This most likely indicates that a release level mismatch exists among nodes in a SYSPLEX. For example, if an ACL had been created for a file by an uplevel node, access attempts to this file from a downlevel node will fail with this message text. Similarly, if an ACL had been created for a file by an uplevel node, and the file system in which it resides has been subsequently mounted by a downlevel node, access attempts to this file will fail with this message text. The text "SECURITY LABEL FAILURE", will be displayed if the user was running with an inappropriate security label, or the resource did not have a security label when one was required. When subcommand is present in the message, "SECLABEL" will be displayed instead of "SECURITY LABEL".

**System action:** RACF returns an error return code to
the invoking system function, which will return an error return code to the application caller or will cause the calling task to abend. See z/OS UNIX System Services Programming: Assembler Callable Services Reference to determine the action of the syscall functions.

**Programmer response:** Provide appropriate information about the failure to the user of your program, based on the function invoked and the return codes received. If "UNABLE TO PROCESS ACL" is displayed, then you must upgrade all nodes in the sysplex to a level of code that supports ACLs. If you require immediate access to the file, try unmounting the file system from the current node, remounting it on an uplevel node, and accessing it from an uplevel node. If a security label failure is indicated, ensure that the resources accessed by your program have the correct security labels.

**Note:** If syscall is LOOKUP or OPEN or the class is DIRSRCH, the problem is most likely access to a directory in the indicated path. See information APAR II12593 to examine the problem.

### ICH408I INSUFFICIENT SECURITY LABEL AUTHORITY

**Explanation:** This error occurs when RACF detects one of the following:

- An attempt to access a resource that has a security label associated with it, and the access cannot be authorized because the requester is running under an inappropriate security label
- An attempt to access a resource that has no security label associated with it and the access cannot be authorized because a security label is required

**System action:** RACF denies the requested access.

**User response:** Log on (or submit the job again) under an appropriate security label and try the access again. For a list of security labels you can specify, enter the following RACF command:

```
SEARCH CLASS(SECLABEL)
```

To find out which security label applies to the task you are currently doing, see your installation security procedures or ask your RACF security administrator.

### ICH408I INSUFFICIENT SECURITY LEVEL/CATEGORY AUTHORITY

**Explanation:** This error occurs when RACF detects an unauthorized attempt to access a RACF-protected resource.

**System action:** RACF denies the requested access.

**User response:** Enter the LISTUSER command to determine the security level and category or see your RACF security administrator.

### ICH408I LOGON/JOB INITIATION - EXCESSIVE PASSWORD OR PASS PHRASE ATTEMPTS

**Explanation:** A user attempted to log on or access the system with passwords, password phrases or both that were not valid more times than allowed by the SETR PASSWORD(REVOKE) setting.

**System action:** RACF prevents the user from accessing the system.

**User response:** Report the exact text of this message to your RACF security administrator.

### ICH408I LOGON/JOB INITIATION - INACTIVE USER HAS BEEN REVOKED

**Explanation:** A user has not logged on, submitted a job or accessed the system for so long that the user ID has become inactive.

**System action:** RACF prevents the user from accessing the system.

**User response:** Report the exact text of this message to your RACF security administrator.

### ICH408I LOGON/JOB INITIATION - INSUFFICIENT SECURITY LABEL AUTHORITY

**Explanation:** This message is issued when RACF detects an attempt to log on or submit a job with a missing or inappropriate security label. This can be issued on SETROPTS multilevel security when dominance check has failed or when the SETROPTS MLACTIVE option is in effect requiring a security label to be specified.

**System action:** RACF prevents the user from logging on or the job from executing.

**User response:** Log on (or submit the job again) under an appropriate security label. For a list of security labels you can specify, see your RACF security administrator.

**Note:** If you can log on (perhaps using a different security label), you can find out which security labels you can use by entering the following RACF command:

```
SEARCH CLASS(SECLABEL)
```

### ICH408I LOGON/JOB INITIATION - INVALID GROUP

**Explanation:** A user attempted to log on or submit a job with an unacceptable group ID specified. The group ID can be a translated group ID.

**System action:** RACF prevents the user from logging on or the job from executing.
ICH408I

User response: Correct any spelling errors in the group ID and try again. If you cannot remember the correct group ID, ask your RACF security administrator to provide you with a valid group ID.

ICH408I LOGON/JOB INITIATION - INVALID OIDCARD

Explanation: A user attempted to log on with an incorrect operator identification card.

System action: RACF prevents the user from logging on.

User response: Attempt to log on again. If the problem persists, report this message to your RACF security administrator.

ICH408I LOGON/JOB INITIATION - INVALID PASSWORD

Explanation: A user attempted to log on or submit a job using a password that is not valid or belongs to a protected user ID.

System action: RACF prevents the user from logging on or the job from executing.

User response: Correct any spelling errors in the password and try again. If you cannot remember your password, ask your RACF security administrator to provide you with a new password.

ICH408I LOGON/JOB INITIATION - INVALID PASSWORD ENTERED AT TERMINAL terminal-id

Explanation: A user attempted to log on with a password that is not valid or belongs to a protected user ID. The attempt was made from terminal terminal-id.

System action: RACF prevents the user from logging on.

User response: Correct any spelling errors in the password and try again. If you cannot remember your password, ask your RACF security administrator to provide you with a new password.

ICH408I LOGON/JOB INITIATION - NOT AUTHORIZED TO SECURITY LABEL

Explanation: You cannot use a particular security label (either for logging on or for initiating a job) unless you have at least READ access authority to the security label profile of that name.

System action: RACF prevents the user from logging on or the job from executing.

User response: Correct any spelling errors in the security label and try again.

Note: If you can log on (perhaps using a different security label), you can find out which security labels you can use by entering the following RACF command:

```
SEARCH CLASS(SECLABEL)
```

RACF Security Administrator Response: If the user should be allowed to use the indicated security label, give the user READ access authority to the security label profile. For example:

```
PERMIT security-label CLASS(SECLABEL)
ID(userid) ACCESS(READ)
```

ICH408I LOGON/JOB INITIATION - NOT AUTHORIZED TO SUBMIT JOB job-name.

Explanation: A job was submitted with the indicated job name, and a check of the submitter user ID done against the JESJOBS profile SUBMIT:xnode:jobname:userid failed, indicating that you are not authorized to submit jobs with the indicated job name, to run on the execution node (xnode), for the specified user ID. You do not have the appropriate access authority to a profile in the JESJOBS class.

System action: RACF prevents the job from executing.

User response: Correct any spelling errors in the job name and try again.

ICH408I LOGON/JOB INITIATION - NOT AUTHORIZED TO {class-name entity-name | TERMINAL/CONSOLE }

Explanation: A user has attempted to:
- log on to the system,
- submit a job,
- perform a transaction, or
- in general, cause some unit of work to be initiated from a RACF defined port of entry,

and is not authorized to do so. Class-name is the port of entry class, such as TERMINAL or JESINPUT, and entity-name is the port to which the user is not authorized, such as a particular terminal or JES node. See z/OS Security Server RACF Data Areas for a list of the RACF port of entry classes and a mapping of the RUTKN data area.
Possible causes of this message are:

1. Security label authorization mismatch
2. User or group authorization insufficient for terminal
3. Access is through universal access authority but NOTERMUACC specified for the connect group
4. Day-of-week or time failure caused by the terminal profile or the user profile

See "Debugging Problems in the RACF Database", in the appendix of [z/OS Security Server RACF Security Administrator's Guide] for extended information about determining the cause of authorization failures. For terminal related problems, also see that appendix for "Authorizing Access to RACF-Protected Terminals".

The original TERMINAL/CONSOLE format of the message is used only when a token is not provided on the request. This format would most likely be issued only on an MVS release before MVS 3.1.3, where tokens are not supported, if the user is trying to log on from a terminal that is not authorized.

**System action:** RACF prevents access to the system from the named port of entry.

**User response:** See your system administrator about obtaining authorization to a specific port of entry.

---

**ICH408I** LOGON/JOB INITIATION - PASS PHRASE IS NOT VALID

**Explanation:** A user attempted to access the system specifying a password phrase that is not valid or specifying a password phrase for a protected user ID.

**System action:** RACF prevents the user from accessing the system.

**User response:** Correct any spelling errors in the password phrase and try again. If you cannot remember your password phrase, ask your RACF security administrator to provide you with a new password phrase.

---

**ICH408I** LOGON/JOB INITIATION - REVOKED USER ACCESS ATTEMPT

**Explanation:** A user who has been revoked has attempted to log on or submit a job.

**System action:** RACF prevents the user from logging on or the job from executing.

**User response:** Report this message to your RACF security administrator.

---

**ICH408I** LOGON/JOB INITIATION - SECURITY LABELS NOT COMPATIBLE.

**Explanation:** Different security labels are associated with the submitter and the job and neither one dominates the other.

**System action:** RACF prevents the job from executing.

**User response:** Ensure that you are using the correct security labels for your logon session and job submission.

---

**ICH408I** LOGON/JOB INITIATION - SUBMITTER IS NOT AUTHORIZED BY USER

**Explanation:** You do not have the appropriate access authority to a profile in the SURROGAT class.

**System action:** RACF prevents the user from logging on or the job from executing.

**User response:** Do one of the following tasks:

1. If you do not intend to submit a job for another user, ensure that the USER parameter on the JOB statement specifies the user ID that you logged on with.
2. If you do intend to submit a job for another user, ask the user whose job you are submitting to ensure that you have the appropriate access authority to their profile in the SURROGAT class. The following command can be used to do this:

   ```
   RLIST SURROGAT userid.SUBMIT AUTHUSER
   ```

   where `userid` is the other user's (job owner's) user ID.

---

**ICH408I** LOGON/JOB INITIATION SUBMITTER IS NOT AUTHORIZED TO SECURITY LABEL

**Explanation:** Submitter does not have authorization to the security label required to run the job. You cannot use a particular security label (either for logging on or for initiating a job) unless you have at least READ access authority to the security label profile of that name.

**Note:** Both user (owner) and submitter of the job must be authorized to security label.

**System action:** RACF prevents the job from executing.

**User response:** Correct any spelling errors in the security label and try again.

**Note:** If you can log on (perhaps using a different security label), you can find out which security labels you can use by entering the following RACF command:

```
SEARCH CLASS(SECLABEL)
```
ICH408I

**System action:** RACF prevents the job from executing.

**User response:** Do one of the following tasks:
- If you do not intend to submit a job for another user, ensure that the USER parameter on the JOB statement specifies the user ID that you logged on with.
- If you do intend to submit a job for another user, ask your RACF security administrator to activate the SURROGAT class.

ICH408I LOGON/JOB INITIATION - SYSTEM NOW REQUIRES MORE AUTHORITY

**Explanation:** The SETROPTS MLQUIET command has been issued. Jobs cannot be initiated, and users cannot logon, until the SETROPTS NOMLQUIET command is issued.

**System action:** Unless the user is trusted, has the SPECIAL attribute, or is the console operator, RACF prevents the user from logging on or the job from executing.

**User response:** Submit your job or attempt to log on again at a later time. If the problem persists, report this message to your RACF security administrator.

ICH408I LOGON/JOB INITIATION - USER SECLABEL NOT COMPATIBLE WITH SERVER

**Explanation:** Different security labels are associated with the user task and the server address space and they are not equivalent. This can occur when:
- The new ACEE is to be anchored at the task level (that is, ACEE= is not specified), but the SECLABEL in the new ACEE is not equivalent to that of the address space ACEE.
- NESTED=YES is specified, but the SECLABEL of the new ACEE is not equivalent to the SECLABEL of the address space ACEE.
- NESTED=COPY was specified, but the SECLABEL of the new ACEE is not equivalent to the SECLABEL of the ACEE that is nested within the address space ACEE.

**System action:** RACROUTE REQUEST=VERIFY processing fails.

**User response:** Ensure that you are using the correct security label for your logon session or job submission, and that you are accessing the correct server.

ICH408I LOGON/JOB INITIATION - USER AT TERMINAL(terminal-id) NOT RACF-DEFINED

**Explanation:** A user who does not have a RACF user profile has attempted to log on to the system.

ICH408I LOGON/JOB INITIATION - WARNING: INSUFFICIENT SECURITY LABEL AUTHORITY

**Explanation:** This error occurs when a user is logging on or a batch job is being initiated, and RACF detects an unauthorized attempt to access a resource that has a security label associated with it. It is issued when MLS WARN is specified, and means that you would have failed a dominance check. For example, this message can be issued if a user attempts to log on at a RACF-protected terminal, and the profile protecting the terminal has a security label specified for it.

**System action:** RACF allows the request to complete.

**User response:** If the security label is misspelled, try again. If you can log on (perhaps using a different security label), you can find out which security labels you can use by entering the following RACF command:

```
SEARCH CLASS(SECLABEL)
```

To find out which security label applies to the task you are currently doing, see your installation security procedures or ask your RACF security administrator.

ICH408I LOGON/JOB INITIATION - WARNING: NOT AUTHORIZED TO SECURITY LABEL

**Explanation:** RACF issues this message when, for example, a user with the SPECIAL attribute specifies a security label such as SYSHIGH does not have at least READ access authority.

**System action:** RACF allows the user to log on or the job to execute.

ICH408I LOGON/JOB INITIATION - WARNING: SECURITY LABEL MISSING

**Explanation:** RACF issues this message when a security label is missing from one of the following:
- The user profile
- A batch job
- A resource profile necessary for logon or job initiation.

and the SETROPTS MLACTIVE(WARNING) option is in effect.

**System action:** RACF allows the user to log on or the job to execute.

**User response:** If a security label is not specified for the profile before the installation puts the SETROPTS MLACTIVE(FAILURES) option into effect, you will not be able to log on or submit the job.
ICH408I  LOGON/JOB INITIATION - WARNING
SECURITY LABELS NOT COMPATIBLE.

**Explanation:** Different security labels are associated with the submitter and the job and neither one dominates the other.

**System action:** RACF allows the job to execute.

**User response:** If you can specify security labels, ensure that you are using the correct security labels for your logon session and job submission. If the system is not in COMPATMODE, this job will fail.

ICH408I  NETWORK JOB ENTRY - JOB FROM NODE node-name NOT AUTHORIZED

**Explanation:** The execution node is protected by the indicated profile in the NODES class (NJE processing). The submitting node or user ID is either not defined to or is not authorized to run on the execution node. The USER and GROUP indicated in the message are the user ID and group ID under which the job was to run (as translated by a profile in the NODES class).

ICH408I  NOT AUTHORIZED TO DEREgISTER DIGITAL CERTIFICATES

**Explanation:** A user attempted to deregister a digital certificate and is not authorized to do so.

**System action:** InitACEE processing ends. RACF prevents the request from completing.

**User response:** See your security administrator.

**RACF Security Administrator Response:** Do the following tasks:

- Make sure that the FACILITY class is active.
- Make sure the IRR.RPKISERV.EXPORT[.ca_domain] resource is defined in the FACILITY class.
- Make sure the IRR.DIGTCERT.EXPORT resource is defined in the FACILITY class.
- Make sure that the user has sufficient authority to both of these resources.

See [z/OS Security Server RACF Security Administrator’s Guide](#) for additional information about the IRR.DIGTCERT.function and IRR.RPKISERV.function resources.

ICH408I  NOT AUTHORIZED TO GENERATE DIGITAL CERTIFICATES

**Explanation:** A user attempted to create a digital certificate using the R_PKIServ callable service function GENCERT, but is not authorized to do so.

**System action:** R_PKIServ processing ends. RACF prevents the request from completing.

**User response:** See your security administrator.

**RACF Security Administrator Response:** Do the following tasks:

- Make sure that the FACILITY class is active.
- Make sure the IRR.RPKISERV.GENCERT resource is defined in the FACILITY class.
- Make sure the IRR.DIGTCERT.GENCERT resource is defined in the FACILITY class.
- Make sure that the user has sufficient authority to all of these resources.

See [z/OS Security Server RACF Security Administrator’s Guide](#) for additional information about the IRR.DIGTCERT.function and IRR.RPKISERV.function resources.

ICH408I  NOT AUTHORIZED PREREGISTER DIGITAL CERTIFICATES

**Explanation:** A user attempted to use the R_PKIServ callable service function, PREREGISTER, to preregister a Simple Certificate Enrollment Protocol (SCEP) client, but is not authorized to do so.

**System action:** R_PKIServ processing ends. RACF prevents the request from completing.

**User response:** See your security administrator.

**RACF Security Administrator Response:** Do the following tasks:

- Make sure that the FACILITY class is active.
- Make sure the IRR.RPKISERV.PKIADMIN resource is defined in the FACILITY class.
ICH408I

- Make sure that the user has UPDATE access to this resource.

See z/OS Security Server RACF Security Administrator’s Guide for additional information about the IRR.RPKISERV function resources.

ICH408I  NOT AUTHORIZED TO REQUEST DIGITAL CERTIFICATES

Explanation: A user attempted to request a PKI Services digital certificate using the R_PKIServ callable service function REQCERT, but is not authorized to do so.

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: See your security administrator.

RACF Security Administrator Response: Do the following tasks:

- Make sure that the FACILITY class is active.
- Make sure the IRR.RPKISERV.REQCERT resource is defined in the FACILITY class.
- Make sure the IRR.DIGTCERT.REQCERT resource is defined in the FACILITY class.
- Make sure that the user has sufficient authority to all of these resources.

See z/OS Security Server RACF Security Administrator’s Guide for additional information about the IRR.DIGTCERT function and IRR.RPKISERV function resources.

ICH408I  NOT AUTHORIZED TO VERIFY DIGITAL CERTIFICATES

Explanation: A user attempted to verify an existing PKI Services digital certificate using the R_PKIServ callable service function VERIFY, but is not authorized to do so.

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: See your security administrator.

RACF Security Administrator Response: Do the following tasks:

- Make sure that the FACILITY class is active.
- Make sure the IRR.RPKISERVVERIFY resource is defined in the FACILITY class.
- Make sure the IRR.DIGTCERTVERIFY resource is defined in the FACILITY class.
- Make sure that the user has sufficient authority to all of these resources.

See z/OS Security Server RACF Security Administrator’s Guide for additional information about the IRR.DIGTCERT function and IRR.RPKISERV function resources.

ICH408I  NOT AUTHORIZED TO REVOKE DIGITAL CERTIFICATES

Explanation: A user attempted to revoke a PKI Services digital certificate using the R_PKIServ callable service function REVOKE, but is not authorized to do so.

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: See your security administrator.

RACF Security Administrator Response: Do the following tasks:

- Make sure that the FACILITY class is active.
- Make sure the IRR.RPKISERV.REVOKE resource is defined in the FACILITY class.
- Make sure the IRR.DIGTCERT.REVOKE resource is defined in the FACILITY class.
- Make sure that the user has sufficient authority to all of these resources.

See z/OS Security Server RACF Security Administrator’s Guide for additional information about the IRR.DIGTCERT function and IRR.RPKISERV function resources.

ICH408I  NOT AUTHORIZED TO REQUEST DIGITAL CERTIFICATES USING SCEP

Explanation: A user attempted to use the R_PKIServ callable service function, SCEPReq, to request a certificate using the Simple Certificate Enrollment Protocol (SCEP), but is not authorized to do so.

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: See your security administrator.

RACF Security Administrator Response: You can give the user access by ensuring:

- The FACILITY class is active.
- The IRR.RPKISERV.SCEPReq resource is defined in the FACILITY class.
- The IRR.DIGTCERT.SCEPReq resource is defined in the FACILITY class.
- The user has sufficient authority to both of these resources.

See z/OS Security Server RACF Security Administrator’s Guide for additional information about the IRR.DIGTCERT function and IRR.RPKISERV function resources.
ICH408I NOT AUTHORIZED TO GENERATE RENEWAL DIGITAL CERTIFICATES

Explanation: A user attempted to generate a PKI Services digital certificate as a renewal for an existing certificate using the R_PKIServ callable service function GENRENEW, but is not authorized to do so.

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: See your security administrator.

RACF Security Administrator Response: Do the following tasks:

• Make sure that the FACILITY class is active.
• Make sure the IRR.RPKISERV.GENRENEW resource is defined in the FACILITY class.
• Make sure the IRR.DIGTCERT.GENRENEW resource is defined in the FACILITY class.
• Make sure the IRR.DIGTCERT.GENCERT resource is defined in the FACILITY class.
• Make sure that the user has sufficient authority to all of these resources.

See z/OS Security Server RACF Security Administrator's Guide for additional information about the IRR.DIGTCERT.function and IRR.RPKISERV.function resources.

ICH408I NOT AUTHORIZED TO REQUEST THE RENEWAL OF DIGITAL CERTIFICATES

Explanation: A user attempted to request the renewal of an existing PKI Services digital certificate using the R_PKIServ callable service function REQRENEW, but is not authorized to do so.

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: See your security administrator.

RACF Security Administrator Response: Do the following tasks:

• Make sure that the FACILITY class is active.
• Make sure the IRR.RPKISERV.REQRENEW resource is defined in the FACILITY class.
• Make sure the IRR.DIGTCERT.REQRENEW resource is defined in the FACILITY class.
• Make sure that the user has sufficient authority to all of these resources.

See z/OS Security Server RACF Security Administrator's Guide for additional information about the IRR.DIGTCERT.function and IRR.RPKISERV.function resources.

ICH408I NOT AUTHORIZED TO LIST DIGITAL CERTIFICATES FOR RECOVERY

Explanation: A user attempted to use the R_PKIServ callable service function, QRECOVER, to list existing PKI Services digital certificates that are candidates for recovery, but is not authorized to do so.

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: See your security administrator.

RACF Security Administrator Response: To avoid receiving this message ensure that:

• The FACILITY class is active.
• The IRR.RPKISERV.QRECOVER[,ca-domain] resource is defined in the FACILITY class.
• The IRR.DIGTCERT.QRECOVER resource is defined in the FACILITY class.
• The user has sufficient authority to all of these resources.

See z/OS Security Server RACF Security Administrator's Guide for more information about the IRR.DIGTCERT.function and IRR.RPKISERV.function resources.

ICH408I NOT AUTHORIZED TO USE OCSP SERVICE

Explanation: A user attempted to verify the certificate status through the PKI OCSP responder using the R_PKIServ callable service function RESPOND, but is not authorized.

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: See your security administrator.

RACF Security Administrator Response: You can give the user access by ensuring:

• The FACILITY class is active.
• The IRR.RPKISERV.RESPOND resource is defined in the FACILITY class.
• The IRR.DIGTCERT.RESPOND resource is defined in the FACILITY class.
• The user has sufficient authority to both of these resources.

See z/OS Security Server RACF Security Administrator's Guide for additional information about the IRR.DIGTCERT.function and IRR.RPKISERV.function resources.
ICH408I NOT AUTHORIZED TO ADMINISTER DIGITAL CERTIFICATES OR CERTIFICATE REQUESTS. [READ | UPDATE] DENIED

Explanation: A user attempted to either query (READ) or modify (UPDATE) one or more PKI Services issued certificates or certificate requests using R_PKIServ callable service, but is not authorized to do so.

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: See your security administrator.

RACF Security Administrator Response: Do the following tasks:
- Make sure that the FACILITY class is active.
- Make sure the IRR.RPKISERV.PKIADMIN resource is defined in the FACILITY class.
- Make sure that the user has sufficient authority to this resource, READ or UPDATE.

See z/OS Security Server RACF Security Administrator’s Guide for additional information about the IRR.DIGTCERT.function and IRR.RPKISERV.function resources.

ICH408I NOT AUTHORIZED TO REGISTER DIGITAL CERTIFICATES

Explanation: A user attempted to register a digital certificate and is not authorized to do so.

System action: InitACEE processing ends. RACF prevents the request from completing.

User response: See your security administrator.

RACF Security Administrator Response: Do the following tasks:
- Make sure that the FACILITY class is active.
- Make sure the IRR.DIGTCERT.ADD profile is defined in the FACILITY class.
- Make sure that the user has sufficient authority to the IRR.DIGTCERT.ADD profile.

See z/OS Security Server RACF Security Administrator’s Guide for more information about automatically assigning UIDs and GIDs. There might also be symptom records in the LOGREC data set that can be used to help diagnose the error. See z/OS Security Server RACF System Programmer’s Guide for more information about possible symptom records.

ICH408I OMVS SEGMENT INCOMPLETELY DEFINED

Explanation: An attempt was made to dub a process and the OMVS segment in the current user's USER profile has no z/OS UNIX user identifier (UID) assigned or the profile for either the user's current connect group or the user's default group does not have an z/OS UNIX group identifier (GID) assigned. Both the current connect group and default group must have GIDs.

System action: RACF returns an error return code to the invoking system function, which will return an error return code to the application caller or will cause the calling task to abend. See z/OS UNIX System Services Programming: Assembler Callable Services Reference to determine the action of the syscall functions.

Programmer response: Provide appropriate information about the failure to the user of your program, based on the function invoked and the return codes received. If you were expecting a UID or GID to be automatically assigned during processing of the BPX.UNIQUE.USER profile in the FACILITY class, the service might have failed for one of the following reasons:
- The BPX.UNIQUE.USER profile is not defined.
- The UNIXPRIV class SHARED.IDS profile is not defined.
- The RACF database has not been converted to stage 3 of application identity mapping.
- The BPX.NEXT.USER profile in the FACILITY class is not defined.
- The BPX.NEXT.USER profile in the FACILITY class does not define a valid UID or GID range.
- The range defined in the BPX.NEXT.USER profile in the FACILITY class has no remaining UID or GID values.

See z/OS Security Server RACF Security Administrator’s Guide for more information about automatically assigning UIDs and GIDs. There might also be symptom records in the LOGREC data set that can be used to help diagnose the error. See z/OS Security Server RACF System Programmer’s Guide for more information about possible symptom records.

ICH408I OMVS SEGMENT NOT DEFINED

Explanation: This error occurs when an attempt is made to dub a process and the current user's USER profile cannot be found in the RACF database or the profile has no OMVS segment.

System action: RACF returns an error return code to the invoking system function, which will return an error return code to the application caller or will cause the calling task to abend. See z/OS UNIX System Services Programming: Assembler Callable Services Reference to determine the action of the syscall functions.

Programmer response: Provide appropriate information about the failure to the user of your program, based on the function invoked and the return codes received. If you were expecting a UID to be automatically assigned during processing of the BPX.UNIQUE.USER profile in the FACILITY class, the service might have failed for one of the following reasons:
- The BPX.UNIQUE.USER profile is not defined.
• The UNIXPRIV class SHARED.IDS profile is not defined.
• The RACF database has not been converted to stage 3 of application identity mapping.
• The BPX.NEXT.USER profile in the FACILITY class is not defined.
• The BPX.NEXT.USER profile in the FACILITY class does not define a valid UID range.
• The range defined in the BPX.NEXT.USER profile in the FACILITY class has no remaining UID values.

See z/OS Security Server RACF Security Administrator’s Guide for more information about automatically assigning UIDs and GIDs. There might also be symptom records in the LOGREC data set that can be used to help diagnose the error. See z/OS Security Server RACF System Programmer’s Guide for more information about possible symptom records.

ICH408I PARTIAL VIOLATION ON COMMAND command
Explanation: This error occurs when RACF detects an unauthorized attempt to use a RACF command that would modify profiles on the RACF database.

ICH408I PROFILE NOT FOUND. IT IS REQUIRED FOR AUTHORIZATION CHECKING.
Explanation: A profile was not found for the general resource, and that general resource’s class has a default return code greater than 4.
User response: Ensure that a profile is created in the general resource class for the resource name indicated in the message before requesting access.

ICH408I PROFILE NOT FOUND. RACFIND WAS SPECIFIED ON THE MACRO.
Explanation: This error occurs when RACF detects an attempt to access a resource that is not protected by a RACF profile, and RACFIND=YES was specified on the RACROUTE REQUEST=AUTH macro.
User response: Ensure that a profile is created to protect this resource, in the class indicated in the message, before requesting access.

ICH408I REMOTE JOB ENTRY - JOB FROM NODE node-name NOT AUTHORIZED
Explanation: A job submitted from the indicated node was not authorized to run on this system. (A UACC of NONE was specified on the NODES profile that applies to this node.)
ICH408I  **RENAME - USER NOT RACF-DEFINED**

Explanation: This error occurs when RACF detects an unauthorized attempt to rename a resource.

System action: RACF prevents the request from completing.

ICH408I  **RENAME - WARNING: RESOURCE NOT PROTECTED**

Explanation: This error occurs when RACF detects an unauthorized attempt to rename a resource.

System action: RACF allows the request to complete.

ICH408I  **RESOURCE NOT PROTECTED**

Explanation: This error occurs when RACF detects an unauthorized attempt to access a resource, but the resource is not protected.

System action: RACF allows the requested access.

ICH408I  **SCCP DIGITAL CERTIFICATE REQUEST REJECTED**

Explanation: A user attempted to use the R_PKIServ callable service function, SCEPReq, to request a certificate using the Simple Certificate Enrollment Protocol (SCEP), but the PKCSReq request is rejected because either the passphrase is missing from the request or it does not match that in the preregistration record.

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: See your security administrator.

RACF Security Administrator Response: Make sure that the passphrase is supplied by the SCEP client and it matches the passphrase when its preregistration record was created.

ICH408I  **SECURITY LABEL MISSING FROM USER, JOB, OR PROFILE**

Explanation: RACF issues this message when a security label is missing from one of the following:

- The user profile
- A batch job
- A resource profile necessary for logon or job initiation.

System action: RACF denies the requested access.

User response: If a line of this message indicates a profile in a RACF class, such as SMITH.CLIST CL(DATABASE) VOL(DS8000), the indicated resource profile is missing a security label.

ICH408I  **WARNING: DATA SET NOT CATALOGED**

Explanation: This error occurs when the SETROPTS CATDSNS(WARNING) option is in effect, and RACF detects an unauthorized attempt to access an uncataloged data set.

System action: RACF allows the requested access.

User response: Catalog the data set and attempt the access again.

Note: If the SETROPTS CATDSNS(FAILURES) command is issued before the data set is cataloged, RACF will fail any subsequent access attempts.

ICH408I  **WARNING: INSUFFICIENT AUTHORITY - TEMPORARY ACCESS ALLOWED**

Explanation: This error occurs when RACF detects an unauthorized attempt to access a RACF-protected resource protected by a profile that is in WARNING mode.

System action: RACF allows the requested access.

ICH408I  **WARNING: INSUFFICIENT SECURITY LABEL AUTHORITY**

Explanation: This error occurs when the SETROPTS MLS(WARNING) option is in effect and RACF detects an attempt to access a resource that would fail because of the security label associated with the resource.

System action: RACF allows the requested access.

User response: Consider logging on again (or submitting the job again) with an appropriate security label. To find out which security label applies to the task you are currently doing, see your installation security procedures or ask your RACF security administrator.

Note: If the SETROPTS MLS(FAILURES) command is issued, RACF will fail any subsequent access attempts.

ICH408I  **WARNING: RESOURCE NOT PROTECTED**

Explanation: This error occurs when RACF detects an unauthorized attempt to access an unprotected resource.

System action: RACF allows the requested access.
ICH408I WARNING: SECURITY LABEL MISSING FROM USER, JOB, OR PROFILE

Explanation: RACF issues this message when a security label is missing from one of the following and the SETROPTS MLACTIVE(WARNING) option is in effect:

- The user profile
- A batch job
- A resource profile necessary for logon or job initiation.

System action: RACF allows the requested access.

User response: If a line of this message indicates a profile in a RACF class, such as SMITH.CLIST CL(DATASET ) VOL(D58000), the indicated resource profile is missing a security label.

ICH409I [abend-code[{yy]}] ABEND DURING request {PROCESSING | PARAMETER VALIDATION}

Explanation: A failure occurred during the RACF processing of the indicated request. If the request indicated in the message is RACROUTE REQUEST=VERIFY (RACINIT), REQUEST=AUTH (RACHECK), REQUEST=DEFINE (RACDEF), or REQUEST=LIST (RACLIST), RACF was processing the SVC related to the request. If the request indicated in the message is DIRAUTH, RACF was processing a directed authorization check request. If the request indicated in the message is IRRSxx00, RACF was processing the indicated callable service.

System action: RACF processing stops.

Operator response: Report the exact text of this message to your system programmer or RACF security administrator, or both, and save the message output.

Programmer response: See “Problem Determination.”

Problem Determination: Try to determine where the abend occurred. RACF, a RACF caller, or other system processing can have caused the abend. If the message says PARAMETER VALIDATION, the RACF caller probably caused the abend.

If the last two digits of the abend are 82, 83, 84, 85, C6, or C7, locate the abend in Chapter 11, “RACF abend codes,” on page 393. The abend description provides additional assistance.

If the last two digits of the abend are not 82, 83, 84, 85, C6, or C7, examine the abend code and analyze the error using general problem determination techniques. The value yy is the contents of Register 15 (in hexadecimal). For system abend and reason codes, see your system codes documentation.

ICH411I MAXIMUM PROFILE SIZE EXCEEDED.
profile-name NOT ALTERED.

Explanation: During RACF processing, an attempt was made to expand the profile indicated in the message. The profile has reached the maximum size that RACF can handle (65,535 bytes); the profile cannot be made larger.

System action: Processing stops.

Operator response: Report this message to the system programmer or the RACF security administrator, or both, and save this output.

Programmer response: The profile has reached the maximum size allowed. If possible, decrease the size of the profile; if that is not possible, split the profile. For example, you can split a group with too many users into several smaller groups.

Destination: Descriptor code is 4. Routing code is 9.

ICH412I RACF DATA AREAS FORCED BELOW THE 16-MEGABYTE LINE.

Explanation: RACF was unable to allocate storage above 16 megabytes because at least one of the installation exit routines does not support 31-bit addressing mode.

Operator response: Notify system programmer.

Programmer response: If possible, change the installation exit routines to support 31-bit addressing mode.

Destination: Descriptor code is 4. Routing code is 2.

ICH414I SMF IS RECORDING ON ITS LAST AVAILABLE DATA SET. WHEN DATA SET FILLS UP, SMF EXIT IEFU29 WILL PLACE THE SYSTEM IN A WAIT STATE.

Explanation: SMF exit routine IEFU29, which stops system operations when all SMF data sets are full, has been installed on your system. This exit routine helps ensure that no SMF data is lost.

System action: Processing continues until the SMF data set fills up. At that time, SMF exit IEFU29 places the system in a wait state.

Operator response: Using installation-defined procedures, archive the SMF data sets that are full. This makes them available for re-use.

Destination: Descriptor code is 2. Routing codes are 1, 2, and 9.
ICH415I • ICH416I

ICH415I  session attempt rejected. reason code =
code, entity netid.luid1. luid2, profile
profile-name, at hh:mm:ss on month, day,
year

Explanation: An attempt by logical unit netid.luid1 to
establish a session with the logical unit luid2 has been
rejected for a security reason. The entity netid.luid1. luid2
was covered by profile profile-name. The message is
routed to the user specified in the NOTIFY field of the
profile.

This message is identical to ICH70005I except that it is
sent to the MVS security console.

System action: The session ends.

Operator response: Notify the RACF security
administrator.

Problem Determination: Check the reason code in the
message for one of the following values:

02 Local LU’s session key will expire in five days
or less

03 Partner LU’s access has been revoked

04 Session key does not match partner LU session
key

05 Partner LU stops the session because of a
security reason

06 Partner LU verification required but no session
key is defined on this system

07 Possible security attack by partner LU

08 Verification was not indicated by partner LU
but a session key exists on this system

09 Verification was indicated by partner LU but a
session key does not exist on this system

10 Failure because of SNA security related
protocol error

11 Failure due profile change during verification

12 A profile was found with an expired session
key

Destination: Descriptor code is 4. Routing codes are 9
and 11.

ICH416I  RACF DETECTED AN INVALID
NON-EGN DATASET PROFILE NAME.
PROFILE profile-name DOES NOT
PROTECT THE INTENDED
RESOURCES.

Explanation: RACF detected a profile that was added
before the enablement of Enhanced Generic Names
(EGN) and that cannot be interpreted as intended
under EGN rules. This message identifies the non-EGN
generic data set profile name. Under EGN rules, the
profile may not protect the resources that it was
defined to protect. If this message is issued during
processing of a SEARCH or LISTDSD GENERIC
request, bad profile names (particularly names 43 and
44 characters in length) may also have been displayed
and the output should be considered unreliable.

For example, suppose the following six generic data set
profiles were defined before turning EGN on:

1 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.**'
2 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.XX.D.DD.*'
3 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.XX.D.D.*'
4 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.DD.*'
5 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.D.*'
6 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.XX.D.DD.*'

Then EGN was enabled and three more generic data set
profiles were defined:

7 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.**'
8 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.DD.*'
9 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.D.*'

A subsequent SEARCH request would display the
following information:

SEARCH CLASS(DATASET)
ICH416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.DD.*
DOES NOT PROTECT THE INTENDED RESOURCES.
ICH416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.D.*
DOES NOT PROTECT THE INTENDED RESOURCES.
ICH416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.DD.*
DOES NOT PROTECT THE INTENDED RESOURCES.
ICH416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.D.*
DOES NOT PROTECT THE INTENDED RESOURCES.
ICH416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME.
PROFILE IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.DD.*
DOES NOT PROTECT THE INTENDED RESOURCES.

Because of RACF command processing, the ICH416I
message may be issued more than once. However, any
time it is issued during a command invocation, the
command output must be considered unreliable. In the
example above, changes in EGN rules caused RACF to
incorrectly interpret non-EGN profiles (1) and (2) as
SEARCH profiles (A) and (B). These profiles no longer
cover the intended resources. Even though names (D)
and (E) appear correct, with no additional characters at
the end, they also do not cover the intended resources
and cause ICH416I messages to be issued. EGN profiles
(7), (8), and (9) were correctly displayed by SEARCH as
(C), (F), and (I). Profiles (G) and (H) follow the same
rules under non-EGN and EGN, so they actually protect what they were intended to protect.

**System action:** RACF processing of the request continues.

**Operator response:** Report this message to the system programmer or the RACF security administrator and save the message output.

**Programmer response:** See problem determination.

**Problem Determination:** This message identifies the bad profile.

An EGN profile, possibly less specific, can be defined to protect the wanted resources; however, the original bad non-EGN profile must still be deleted to prevent further ICH416I messages.

To delete bad profiles:

1. Use SETROPTS NOEGN to temporarily disable EGN. During this time, there should be no other system activity, in order to prevent the creation of generic profiles that can result in additional problems. Under normal circumstances, it is not recommended that EGN be turned off after it is turned on.

2. Use SEARCH GENERIC CLIST NOMASK NOLIST to create a CLIST containing generic data set profile names.

3. Edit the CLIST to find 42- and 43-character names ending in ‘.*’.

4. Delete the profiles found.

5. Use SETROPTS EGN to re-enable EGN.

6. Define profiles according to EGN rules that protect the resources intended to be protected by the non-EGN profile names.

**Destination:** Descriptor code is 4. Routing codes are 9 and 11. Routing code 11 is only used when a TSO environment is not in effect.

ICH417I  **THE ENVIRONMENT IS NOT CONTROLLED. CONDITIONAL ACCESS LIST BYPASSED FOR DATA SET dsname**

**Explanation:** The profile that protects the data set has a conditional access list that would have granted access, but RACF did not use it because the environment is not controlled.

**System action:** RACF denies the requested access.

**User response:** Check for additional error messages describing the reason the environment is not controlled and take appropriate action to ensure that the environment is controlled.

**Destination:** Descriptor code is 6. Routing code is 9 and 11.
ICH420I  PROGRAM program-name, FROM 
[[LIBRARY dsname] | LPA | JPA | 
IDENTIFY ] CAUSED THE 
ENVIRONMENT TO BECOME 
UNCONTROLLED.

Explanation: You have previously loaded 
program-name into your environment. This program is 
not protected by a RACF profile in the PROGRAM 
class. The presence of this program has caused the 
environment to be marked uncontrolled.

User response: Try to access this resource in an 
environment that does not contain program-name. If this 
is not possible, report the message to your security 
administrator.

RACF Security Administrator Response: Define a 
profile in the PROGRAM class to protect the program 
indicated by the message.

If IDENTIFY is specified, a program that is not defined 
to RACF in the PROGRAM class has used the 
IDENTIFY service to define program-name as an entry 
point. In this case, the initial program must be a MAIN 
or BASIC program if it is in ENHANCED mode and 
you need to use the EXECUTE control or Program 
Access to Data Sets (PADS). The initial program must 
at least be defined to RACF for the other functions that 
require a clean environment.

Destination: Descriptor code is 6. Routing code is 9 
and 11.

ICH421I  REASON FOR UNCONTROLLED 
ENVIRONMENT IS NOT KNOWN.

Explanation: RACF cannot determine why the 
environment is not controlled. This indicates that a 
program marked the environment uncontrolled without 
using the environment service, IRRENS00.

User response: If you are in a TSO/E environment, 
logoff and logon again or use TSOEXEC to create a 
new controlled environment, and then try to access this 
resource. If the problem continues, report the message 
to your security administrator.

RACF Security Administrator Response: Check 
PROGRAM class definitions and ensure that the user 
should have access to the resource when accessing it as 
attempted. Report the problem to the IBM support 
center.

Destination: Descriptor code is 6. Routing code is 9 
and 11.

ICH422I  THE ENVIRONMENT CANNOT 
BECOME UNCONTROLLED.

Explanation: The IRRENS00 service received a request 
to mark the environment uncontrolled. This request cannot be satisfied because the environment must 
remain controlled to maintain system security.

System action: RACF denies the request.

User response: Check for additional error messages 
describing the reason the environment cannot become 
uncontrolled and take the action specified for the 
additional messages. Or, try in a different environment 
that does not contain sensitive data or programs that 
require the environment to be kept controlled.

Destination: Descriptor code is 6. Routing code is 9 
and 11.

ICH423I  RACF EXECUTE-CONTROLLED 
PROGRAMS ARE ACTIVE: 
program-name1, program-name2, 
program-name3 ...

Explanation: The IRRENS00 service received a request 
to mark the environment uncontrolled, and has 
determined that it cannot satisfy that request because of 
the presence of execute-controlled programs. Only the 
first 20 programs found are listed in the message.

If two ICH423I messages are received, then there are 
currently more than one execute-controlled programs 
avtive in the environment, and the environment was 
originally marked keep-controlled because of an 
execute-controlled program.

User response: Report the message to your security 
administrator.

RACF Security Administrator Response: The user has 
attempted a function that would make his environment 
uncontrolled. RACF failed the request because there are 
execute-controlled programs running in his 
environment. Determine if the user should be allowed 
to perform this action in his current environment. If so, 
correct the RACF PROGRAM and DATASET class 
definitions to allow access.

Destination: Descriptor code is 6. Routing code is 9 
and 11.

ICH424I  DATA SETS OPENED USING RACF 
WHEN(PROGRAM(...)) ARE STILL 
OPEN: dsname1, dsname2, dsname3 ...

Explanation: The IRRENS00 service received a request 
to mark the environment uncontrolled. It cannot satisfy 
that request because program-accessed data sets are 
already open in the environment. Only the first 4 data 
sets found are listed in the message.

User response: Close the data sets listed in the 
message, and try again.

Destination: Descriptor code is 6. Routing code is 9 
and 11.
**ICH425I**  UNIX SYSTEM SERVICES MUST KEEP THE ENVIRONMENT CONTROLLED.

**Explanation:** The IRRENS00 service received a request to mark the environment uncontrolled. It cannot satisfy that request because z/OS UNIX has requested the environment be kept controlled.

**User response:** Check for additional error messages with the message prefix BPX describing the reason the environment cannot become uncontrolled and take the action specified for the additional messages. Or, try in a different environment that does not contain sensitive data or programs that require the environment be kept controlled.

**Destination:** Descriptor code is 6. Routing code is 9 and 11.

---

**ICH426I**  NON-MAIN PROGRAM IS IN CONTROL. CONDITIONAL ACCESS LIST BYPASSED FOR DATA SET **dsname**

**Explanation:** The profile that protects the data set has a conditional access list that would have granted access by using the WHEN(PROGRAM), but RACF did not use it because ENHANCED PGMSECURITY mode is in effect (FACILITY profile IRR.PGMSECURITY exists with an APPLDATA value of ENHANCED) and the environment was established by a program that did not have the MAIN attribute. This would normally cause RACF to reject use of the conditional access list entry, but RACF has allowed it because the administrator enabled WARNING mode for ENHANCED PGMSECURITY. This access would have failed if the administrator had instead enabled ENHANCED mode of PGMSECURITY.

**System action:** RACF allows the requested access, but issues the warning message.

**RACF Security Administrator Response:** Or user response:

Verify that the first program executed in this execution environment (jobstep, or specified on TSOEXEC command or by way of the IKJEFTSR service) has a specific PROGRAM profile that specifies the MAIN attribute. If not, you may redefine the program to have MAIN, if it is a program that you trust to maintain the environment properly for using conditional access, or you may change the way you invoke the program (for example, under TSO consider invoking the program by using the TSOEXEC command), or you may change the option to BASIC PGMSECURITY mode, or you may define the program as one that needs BASIC PGMSECURITY mode by defining it with a specific PROGRAM profile that has an APPLDATA value of BASIC. Using a PROGRAM profile with BASIC provides less security but may be necessary for some programs where you cannot use TSOEXEC.

Do not enable the failure mode of ENHANCED PGMSECURITY before you resolve this message, or you will cause accesses to fail.

**Destination:** Descriptor code is 6. Routing codes are 9 and 11.

---

**ICH427I**  NON-MAIN PROGRAM IS IN CONTROL. TEMPORARY USE OF CONDITIONAL ACCESS LIST ALLOWED FOR DATA SET **dsname**

**Explanation:** The profile that protects the data set has a conditional access list that would grant access by way of the WHEN(PROGRAM) if BASIC PGMSECURITY was in effect. However, ENHANCED PGMSECURITY is in effect and the environment was established by a program that did not have the MAIN attribute. This would normally cause RACF to reject use of the conditional access list entry, but RACF has allowed it because the administrator enabled WARNING mode for ENHANCED PGMSECURITY. This access would have failed if the administrator had instead enabled ENHANCED mode of PGMSECURITY.

**System action:** RACF allows the requested access, but issues the warning message.

**RACF Security Administrator Response:** Or user response:

Check for additional messages that provide further details, such as ICH428I. Verify that the first program executed in this execution environment (jobstep, or specified on TSOEXEC command or by way of the IKJEFTSR service) has a specific PROGRAM profile that specifies the MAIN attribute. If not, you may redefine the program to have MAIN, if it is a program that you trust to maintain the environment properly for using conditional access, or you may change the way you invoke the program (for example, under TSO consider invoking the program by using the TSOEXEC command), or you may change the option to BASIC PGMSECURITY mode, or you may define the program as one that needs BASIC PGMSECURITY mode by defining it with a specific PROGRAM profile that has an APPLDATA value of BASIC. Using a PROGRAM profile with BASIC provides less security but may be necessary for some programs where you cannot use TSOEXEC.

Do not enable the failure mode of ENHANCED PGMSECURITY before you resolve this message, or you will cause accesses to fail.

**Destination:** Descriptor code is 6. Routing codes are 9 and 11.

---

**ICH428I**  PROGRAM **program-name** FROM { **library-name** | LPA | JPA | IDENTIFY} ESTABLISHED THE CURRENT EXECUTION ENVIRONMENT

**Explanation:** The named program from the specified library (or from the Link Pack or Job Pack or IDENTIFY service) was the first program executed in this jobstep or, if applicable, in this TSO service routine (IKJEFTSR, TSOEXEC) environment. This program is not defined to RACF as a MAIN or BASIC program through a PROGRAM profile with an APPLDATA of MAIN, or BASIC therefore, in an ENHANCED PGMSECURITY environment, is not trusted to provide...
a safe environment for the use of program access to
data sets or SERVAUTH class (PADS, or WHEN(PGM)
conditional access list entries) for loading
EXECUTE-controlled programs, nor for some UNIX
System Services functions. RACF provides the name
and location of the program to help you diagnose the
problems reported in other messages issued by RACF
or UNIX System Services.

System action: None. Also, see other messages issued
by RACF or UNIX System Services to see the system
action that occurred.

RACF Security Administrator Response: Or user
Response:
Examine the other messages you received and take the
appropriate actions indicated for those messages.

Destination: Descriptor code is 6. Routing codes are 9
and 11.

ICH429I NON-MAIN PROGRAM IS IN
CONTROL. ATTEMPT TO LOAD
PROGRAM program-name FROM
LIBRARY library-name FAILED.

Explanation: The user has only EXECUTE authority to
the named program, by way of the PROGRAM profiles
or the DATASET profile for the library. RACF cannot
allow use of the program because ENHANCED
PGMSECURITY mode is in effect (FACILITY profile
IRR.PGMSECURITY exists with an
APPLDATA value of ENHANCED) and the
environment was established by a program that did not
have the MAIN attribute. This would normally cause
RACF to prohibit use of the program by this user, but
RACF has allowed it because the administrator enabled
the WARNING mode for ENHANCED PGMSECURITY.
This access would have failed if the administrator had
instead enabled the ENHANCED mode of
PGMSECURITY.

System action: Access is denied by RACF.

RACF Security Administrator Response: Or user
Response:
Check for additional messages that provide further
details, such as ICH428I. Verify that the first program
executed in this execution environment (jobstep, or
specified on TSOEXEC command or by way of
IKJEFTSR service) has a PROGRAM profile that
specifies the MAIN attribute. If not, you may redefine
the program to have MAIN, if it is a program that you
trust to maintain the environment properly for using
conditional access, or you may change the way you
invoke the program (for example, under TSO consider
invoking the program by way of the TSOEXEC
command), or you may change the option to BASIC
PGMSECURITY mode, or you may define the program
as one that needs BASIC PGMSECURITY mode by
defining it with a specific PROGRAM profile that has
an APPLDATA value of BASIC. Using a PROGRAM
profile with BASIC provides less security but may be
necessary for some programs where you cannot use
TSOEXEC.

Do not enable the failure mode of ENHANCED
PGMSECURITY before you resolve this message, or
you will cause accesses to fail.

Destination: Descriptor code is 6. Routing codes are 9
and 11.

ICH431I THE ENVIRONMENT IS NOT
CONTROLLED. CONDITIONAL
ACCESS LIST BYPASSED FOR
class-name resource-name .

Explanation: The profile that protects the resource has
a conditional access list that would have granted
access, but RACF did not use it because the
environment is not program controlled.

System action: RACF denies the requested access.
**User response:** Check for additional error messages describing the reason the environment is not controlled and take the appropriate action to ensure that the environment is controlled.

**Destination:** Descriptor code is 6. Routing codes are 9 and 11.

---

**ICH432I**  
**CONDITIONAL ACCESS LIST FOR**  
*class-name resource-name*  
**DID NOT**  
**GRANT AUTHORITY TO**  
**PROGRAM(S):**  
*program-name*  
*program-name2*  
*program-name3*

**Explanation:** The profile protecting the resource has a conditional access list, but it did not contain the correct program or programs on the access list to grant authority to the resource. The program-name is the currently executing program and does not appear in the conditional access list. Only the first 11 programs found are listed in the message. If the program is an executable file loaded from the z/FS or shared file system, the program name is not available to RACF. The message will contain *EXEFILE as the program name when the program is an executable file.

**System action:** RACF denies the requested access.

**User response:** Permit the correct programs to the conditional access list of the profile covering the resource, or ask your security administrator to do so.

**Destination:** Descriptor code is 6. Routing codes are 9 and 11.

---

**ICH433I**  
**NON-MAIN PROGRAM IS IN**  
**CONTROL. CONDITIONAL ACCESS**  
**LIST BYPASSED FOR**  
*class-name resource-name* .

**Explanation:** The profile protecting the resource has a conditional access list that would have granted access by way of the WHEN(PROGRAM), but RACF did not use it because ENHANCED PGMSECURITY mode is in effect (FACILITY profile IRR.PGMSECURITY exists with an APPLDATA value of ENHANCED) and the environment was established by a program that did not have the MAIN attribute.

**System action:** Access is denied by RACF.

**RACF Security Administrator Response:** Check for additional messages that provide further details. Verify that the first program executed in this execution environment (jobstep, or specified on TSOEXEC command or by way of the IKJEFTSR service) has a specific PROGRAM profile that specifies the MAIN attribute. If not, you may redefine the program to have MAIN, if it is a program that you trust to maintain the environment properly for using conditional access, or you may change the way you invoke the program (for example, under TSO consider invoking the program by way of the TSOEXEC command), or you may change the system to run in BASIC PGMSECURITY mode, or you may define the program as one that needs BASIC PGMSECURITY mode by defining it with a specific PROGRAM profile that has an APPLDATA value of BASIC. Using a PROGRAM profile with BASIC provides less security but may be necessary for some programs where you cannot use TSOEXEC.

**Destination:** Descriptor code is 6. Routing codes are 9 and 11.

---

**ICH434I**  
**NON-MAIN PROGRAM IS IN**  
**CONTROL. TEMPORARY USE OF**  
**CONDITIONAL ACCESS LIST**  
**ALLOWED FOR**  
*class-name resource-name* .

**Explanation:** The profile protecting the resource has a conditional access list that would grant access by way of the WHEN(PROGRAM) if BASIC PGMSECURITY was in effect. However, ENHANCED PGMSECURITY is in effect and the environment was established by a program that did not have the MAIN attribute. This would normally cause RACF to reject use of the conditional access list entry, but RACF has allowed it because the administrator enabled WARNING mode for ENHANCED PGMSECURITY. This access would have failed if the administrator had instead enabled ENHANCED mode of PGMSECURITY.

**System action:** RACF allows the requested access, but issues the warning message.

**RACF Security Administrator Response:** Verify that the first program executed in this execution environment (jobstep, or specified on TSOEXEC command) has a PROGRAM profile that specifies the MAIN attribute. If not, you may redefine the program to have MAIN, or you may change the option to BASIC PGMSECURITY mode, or you may define the program as one that needs BASIC PGMSECURITY mode by defining it with a specific PROGRAM profile that has an APPLDATA value of BASIC. Using a PROGRAM profile with BASIC provides less security but may be necessary for some programs where you cannot use TSOEXEC. Do not enable the failure mode of ENHANCED PGMSECURITY before you resolve this message, or you will cause accesses to fail.

**Destination:** Descriptor code is 6. Routing codes are 9 and 11.

---

**ICH435I**  
*class-name resource-name*  
**ACCESS**  
**WITH WHEN(PROGRAM(...)):**  
*resource-name* .

**Explanation:** The IRRENS00 service received a request to mark the environment uncontrolled, and has determined that it cannot satisfy that request because of
ICH440I • ICH442I

the presence of a resource accessed by way of the conditional access list. Only the first resource accessed is listed in the message.

User response: Report the message to your security administrator.

RACF Security Administrator Response: The user has attempted a function that would make his environment uncontrolled. RACF failed the request because the environment cannot become uncontrolled. Determine if the user should be allowed to perform this action in his current environment. If so, correct the RACF PROGRAM, DATASET, and SERVAUTH class definitions to allow access.

Destination: Descriptor code is 6. Routing codes are 9 and 11.

ICH440I Program signature error retcode/rsncode for program program-name in library library-name. The program was not loaded.

Explanation: RACF detected an error with the cryptographic signature of the identified program. A subsequent message is issued that provides more information about this error.

Note: This message is only issued if the audit specifications, in the SIGVER segment of the PROGRAM profile, result in the condition being audited.

System action: The load fails.

RACF Security Administrator Response: See the subsequent message for more information. Additional information is provided in the return and reason code displayed in the message. These codes are from the VERFINAL function of the R_PgmSignVer (IRRPS00) callable service and descriptions for these codes can be found in [z/OS Security Server RACF Callable Services]. A reason code greater than or equal to 100 might indicate a setup problem with the verification key ring, which can be fixed by the security administrator. Other reason codes must be reported to the provider of the failing module.

Destination: Descriptor code is 6. Routing codes are 9 and 11.

ICH442I The digital signature appears to be valid but the root signer is not trusted.

Explanation: The digital signature in the program is correct, but the root CA certificate of the certificate chain contained with the signature has not been designated as trusted, or the setup configuration is preventing RACF from being able to determine the trusted status. This message can result from any of the following conditions:

• The IRR.PROGRAM.SIGNATURE.VERIFICATION profile is not defined in the FACILITY class.
• The APPLDATA field of the IRR.PROGRAM.SIGNATURE.VERIFICATION profile is missing or incorrect. (The APPLDATA is used to identify the key ring that contains the trusted root certificates.)
• The APPLDATA identifies a key ring that does not exist.
• The root CA certificate of the certificate chain contained with the signature has not been added to the specified key ring, or has been added with the NOTRUST flag.
• The root CA certificate in the certificate chain contained with the signature has the NOTRUST flag on.

Notes:
1. The program name is identified in message ICH440I or ICH441I. One of these messages precedes this message.
2. This message is only issued if the audit specifications, in the SIGVER segment of the PROGRAM profile, result in the specific condition being audited.

3. There might also be diagnostic information in a LOGREC record.

**System action:** If message ICH441I precedes this message, the program load continues. If message ICH440I precedes this message, the load fails.

**RACF Security Administrator Response:** If you trust the certificate chain associated with the signed program, you must place the root CA certificate into the appropriate key ring.

You can temporarily bypass this error in any of the following ways:

- If you have specified FAILLOAD(ANYBAD) in the SIGVER segment of the RACF PROGRAM class profile that protects this program, then specify FAILLOAD(BADSIGONLY). This change enables the program to continue.
- Specify SIGAUDIT(BADSIGONLY) or NOSIGAUDIT to stop this message being issued for this program again.
- Remove the SIGVER segment from the PROGRAM class profile.
- Delete the PROGRAM class profile if it is not being used to restrict or audit access to the program.

**Note:** The current security policy has flagged this condition as an error. Bypassing the error prevents this message from being issued when the program is loaded, but reduces system security and does not resolve the problem. Once you have resolved the problem, revisit your FAILLOAD and SIGAUDIT settings.

**Destination:** Descriptor code is 6. Routing codes are 9 and 11.

---

### ICH443I

**Explanation:** The digital signature in the program does not match the hash of the program computed by RACF. This message indicates that the program has been either modified since it was created, or that it was not properly signed.

**Notes:**

1. The program name is identified in message ICH440I or ICH441I. One of these messages precedes this message.
2. This message is only issued if the audit specifications, in the SIGVER segment of the PROGRAM profile, result in the specific condition being audited.
3. There might also be diagnostic information in a LOGREC record.

**System action:** If message ICH441I precedes this message, the program load continues. If message ICH440I precedes this message, the load fails.

**RACF Security Administrator Response:** Save the current program, and then replace the program with a copy from the installation media. If replacing the program with a copy from the installation media does not resolve the problem, replace the program with a copy from program provider.

You can temporarily bypass this error in any of the following ways:

- If the load fails, change the SIGVER segment of the RACF PROGRAM class profile that protects this program to specify FAILLOAD(NEVER). This change enables the program to continue.
- Specify SIGAUDIT(NONE) or NOSIGAUDIT to stop this message being issued for this program again.
- Remove the SIGVER segment from the PROGRAM class profile.
- Delete the PROGRAM class profile if it is not being used to restrict or audit access to the program.

**Note:** The current security policy has flagged this condition as an error. Bypassing the error prevents this message from being issued when the program is loaded, but reduces system security and does not resolve the problem. Once you have resolved the problem, revisit your FAILLOAD and SIGAUDIT settings.

**Destination:** Descriptor code is 6. Routing codes are 9 and 11.

---

### ICH444I

**Explanation:** When a program is signed during the bind process, the program object contains a digital signature and the digital certificate chain for the user who performed the program bind. This message indicates that the digital certificate chain is incorrect.

The reason code in this message indicates the reason for the failure. This reason code originates from the R_PgmSignVer callable service (IRRSPS00), which is called to verify the signature and certificate chain when the program is loaded. In z/OS Security Server RACF Callable Services, there is a specific set of return and reason codes documented for function code X'0007' (VERFINAL). The relevant reason codes are documented under SAF return code 8 and RACF return code 16.

**Notes:**

1. The program name is identified in message ICH440I or ICH441I. One of these messages precedes this message.
2. This message is only issued if the audit specifications, in the SIGVER segment of the PROGRAM profile, result in the specific condition being audited.

3. There might also be diagnostic information in a LOGREC record.

**System action:** If message ICH441I precedes this message, the program load continues. If message ICH440I precedes this message, the load fails.

**RACF Security Administrator Response:** Inform the provider of the program with the information in this message. Either the program was not built correctly, or it has been modified. A new copy of the module with the correct signature and certificate chain is required.

You can temporarily bypass this error in any of the following ways:

- If the load fails, change the SIGVER segment of the RACF PROGRAM class profile that protects this program to specify FAILLOAD(NEVER). This change enables the program to continue.
- Specify SIGAUDIT(NONE) or NOSIGAUDIT to stop this message being issued for this program again.
- Remove the SIGVER segment from the PROGRAM class profile.
- Delete the PROGRAM class profile if it is not being used to restrict or audit access to the program.

**Note:** The current security policy has flagged this condition as an error. Bypassing the error prevents this message from being issued when the program is loaded, but reduces system security and does not resolve the problem. Once you have resolved the problem, revisit your FAILLOAD and SIGAUDIT settings.

**Destination:** Descriptor code is 6. Routing codes are 9 and 11.

---

**ICH445I** A digital signature is required but the program is not signed.

**Explanation:** The SIGVER segment of the RACF PROGRAM class profile protecting this program specifies SIGREQUIRED(YES). This indicates that this program requires a signature, but the program is not digitally signed.

**Notes:**

1. The program name is identified in message ICH440I or ICH441I. One of these messages precedes this message.
2. This message is issued only if the audit specifications in the SIGVER segment of the PROGRAM profile result in the specific condition being audited.

**System action:** The load fails.

**RACF Security Administrator Response:** Contact the provider of the program and request a digitally signed version of this program.

You can temporarily bypass this error in any of the following ways:

- If the load fails, change the SIGVER segment of the RACF PROGRAM class profile that protects this program to specify SIGREQUIRED(NO). This change enables the program to continue.
- Specify SIGAUDIT(NONE) or NOSIGAUDIT to stop this message being issued for this program again.
- Remove the SIGVER segment from the PROGRAM class profile.
- Delete the PROGRAM class profile if it is not being used to restrict or audit access to the program.

**Note:** The current security policy has flagged this condition as an error. Bypassing the error prevents this message from being issued when the program is loaded, but reduces system security and does not resolve the problem. Once you have resolved the problem, revisit your FAILLOAD and SIGAUDIT settings.

**Destination:** Descriptor code is 6. Routing codes are 9 and 11.

---

**ICH446I** The digital signature has been removed from the program.

**Explanation:** The PSDE directory indicates that the program member is digitally signed, but the program does not contain a digital signature. This message indicates that the program has been modified since it was created.

**Notes:**

1. The program name is identified in the ICH440I message, which precedes this one.
2. This message is issued only if the audit specifications in the SIGVER segment of the PROGRAM profile result in the specific condition being audited.

**System action:** The load fails.

**RACF Security Administrator Response:** Save the current program, and then replace the program with a copy from the installation media. If replacing the program with a copy from the installation media does not resolve the problem, replace the program with a copy from program provider.

You can temporarily bypass this error in any of the following ways:

- Remove the SIGVER segment from the PROGRAM class profile.
- Delete the PROGRAM class profile if it is not being used to restrict or audit access to the program.
ICH447I  RACF was unable to load and verify the program verification module.

Explanation: An error occurred while RACF was attempting to load and verify the program verification module (IRRPVERS).

System action: No program signatures are verified until the error is resolved and the program verification module is loaded.

RACF Security Administrator Response: This message might have the following preceding messages:
- Either ICH451I, or
- Three of the following messages:
  1. ICH440I
  2. ICH442I, ICH443I, ICH444I, ICH445I, or ICH446I
  3. ICH451I

See these message descriptions and resolve the problem. After the problem is resolved, notify your system programmer to run the IRRVERLD program to load the program verification module (IRRPVERS).

If this message is not preceded by other messages, there might be a problem in the PROGRAM class profile covering resource IRRPVERS. Ensure that this profile is correctly defined, and that the data set name in the member list points to the data set that contains the program verification module (IRRPVERS). You must also ensure that the SIGVER segment of this profile is defined, and does not contains the following values:
- FAILLOAD(NEVER)
- SIGAUDIT(NONE)
- SIGREQUIRED(NO)

If the IRRPVERS profile in the PROGRAM class is correctly defined, ensure that the SETR WHEN(PROGRAM) option is set and refreshed.

Destination: Descriptor code is 6. Routing codes are 9 and 11.

ICH448I  RACF program signature verification module is loaded. Program signature verification is available on this system.

Explanation: The RACF initialization process or the IRRVERLD program has loaded and verified the program verification module (IRRPVERS). Program signature verification is available on this system.

System action: Subsequent program verification operations complete normally.

RACF Security Administrator Response: None

Destination: Descriptor code is 6. Routing codes are 9 and 11.

ICH450I The RACF program verification module is not loaded. Program signature verification is not available.

Explanation: An attempt was made to load a signed program that is covered by a profile in the PROGRAM class. The profile indicates that the signature is to be verified. However, the program verification module (IRRPVERS) has not been loaded. Program verification is only available when the program verification module (IRRPVERS) has been loaded.

Note: The program name is identified in message ICH440I or ICH441I. One of these messages precedes this message.

System action: Depending on the program configuration options set in the SIGVER segment of the PROGRAM profile, the attempt to load the program either succeeds or fails.

RACF Security Administrator Response: Notify your system programmer to run the IRRVERLD program to load and verify the program verification module (IRRPVERS).

Destination: Descriptor code is 6. Routing codes are 9 and 11.
ICH451I  RACF encountered an error while attempting to load the program verification module. Operation code = X’a’a’. Return code X’b b b b’ and Reason code X’c c c c’. Supplemental diagnostic code 1 = X’d d d d d d d d’’. Supplemental diagnostic code 2 = X’e e e e e e e’’. Supplemental diagnostic code 3 = X’f f f f f f f f’’. Supplemental diagnostic code 4 = X’g g g g g g g g’’. Supplemental diagnostic code 5 = X’h h h h h h h h’’.

Explanation: A system service failed while RACF attempted to load the program verification module (IRRPVERS). The failing system service, return code, and reason code, are defined in the following table:

<table>
<thead>
<tr>
<th>Operation code (X’a’a’)</th>
<th>Failing system service</th>
<th>Return code</th>
<th>Reason code</th>
</tr>
</thead>
<tbody>
<tr>
<td>X’01’</td>
<td>IEANTCR</td>
<td>X’b b b b’’</td>
<td>X’c c c c’’</td>
</tr>
<tr>
<td>X’02’</td>
<td>IEANTRT</td>
<td>X’b b b b’’</td>
<td>X’c c c c’’</td>
</tr>
<tr>
<td>X’03’</td>
<td>CSVDYLPA REQUEST=ADD</td>
<td>X’b b b b’’</td>
<td>X’c c c c’’</td>
</tr>
<tr>
<td>X’04’</td>
<td>BLDL</td>
<td>X’b b b b’’</td>
<td>X’c c c c’’</td>
</tr>
<tr>
<td>X’05’</td>
<td>STORAGE OBTAIN</td>
<td>X’b b b b’’</td>
<td>X’c c c c’’</td>
</tr>
<tr>
<td>X’06’</td>
<td>LOAD</td>
<td>X’b b b b’’</td>
<td>X’c c c c’’</td>
</tr>
</tbody>
</table>

Note: The return code and reason code from the failing service are included in this message.

If the operation code is X’03’, the supplemental diagnostic codes have values. You can use the supplemental diagnostic values in the following table to determine the problem:

<table>
<thead>
<tr>
<th>Supplemental Diagnostic Code</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>LpmeaOutputFlags</td>
</tr>
<tr>
<td>2</td>
<td>LpmeaRetcode</td>
</tr>
<tr>
<td>3</td>
<td>LpmeaRsncode</td>
</tr>
<tr>
<td>4</td>
<td>LpmeaAbendCode</td>
</tr>
<tr>
<td>5</td>
<td>LpmeaAbendRsnCode</td>
</tr>
</tbody>
</table>

See the CSVDYLPA ADD service in [z/OS MVS Programming: Authorized Assembler Services Reference ALE-DYN](https://pic.dhe.ibm.com/infocenter/zos/v1r13/preauth/a000003c.pdf) for more information about the supplemental diagnostic codes.

If the operation code is not X’03’, the supplemental codes have no meaning.

System action: No program signatures are verified until the error is resolved and the program verification module is loaded. Depending on the signature verification options set in the SIGVER segment of the PROGRAM profile, the attempt to load the program might fail.

RACF Security Administrator Response: Determine the reason for the system service failure using the return codes and resolve the problem. After the problem is resolved, notify your system programmer to run the IRRVERLD program to load the program verification module (IRRPVERS).

Destination: Descriptor code is 6. Routing codes are 9 and 11.

ICH452I  The RACF program verification module self-test failed. Program signature verification is not available.

Explanation: The program verification module (IRRPVERS) encountered an error while performing a self test during an attempt to initialize.

System action: No program signatures are verified until the error is resolved and the program verification module is loaded. A record is added to LOGREC with additional diagnostic information.

RACF Security Administrator Response: Contact IBM support.

Destination: Descriptor code is 6. Routing codes are 9 and 11.
RACF initialization messages

ICH500I  I/O ERROR DURING RACF INITIALIZATION [[PRIMARY | BACKUP] RACF DATA SET SEQUENCE nnn, dsname]

Explanation: During RACF initialization, an I/O error occurred on the RACF database.

System action: The system issues ICH502A following this message, then waits for the operator's reply.

Operator response: Notify your system programmer.

Programmer response: Determine if the device or volume used for the RACF database is functioning properly.

Destination: Descriptor code is 4. Routing code is 2.

ICH501I --RACF IS NOT ACTIVE.--

Explanation: During RACF initialization or sysplex communication processing, either a RACF error or a system error occurred.

System action: RACF becomes inactive. If RACF had joined the sysplex data sharing group, it leaves the group. RACF allows access to the following:
- Resources accessed by started tasks that are marked as privileged or trusted in the RACF started procedures table (ICHRIN03)
- A user’s own data sets
- Any other data sets to which the operator allows access
- Any general resource for which the access authorization is done by way of RACHECK, and to which the operator allows access
- All general resources for which the access authorization is done by way of RACROUTE REQUEST=AUTH

Operator response: Notify your system programmer.

Programmer response: Correct the problem and IPL again.

Problem Determination: A message (either ICH505A, ICH564A, ICH565A, ICH566A, ICH567A, ICH568A, ICH569A, ICH570A, ICH571A, ICH572A, ICH573A, ICH574A, ICH575A, or ICH576A) precedes this message if the error occurred during initialization and indicates the cause of the error. For sysplex communication errors, there is an abend and an associated dump.

Note: In previous releases, the following messages preceded this message: ICH511I, ICH512I, ICH517I, ICH518I, ICH523I, ICH526I, ICH528I, ICH537I, ICH549I, ICH550I, ICH551I, or ICH553I.

ICH502A SPECIFY NAME FOR [PRIMARY | BACKUP] RACF DATA SET SEQUENCE nnn OR ‘NONE’

Explanation: The data set name table (ICHRDSNT) indicates that a primary (or backup) database is requested for the sequence number nnn. However, either no data set name was given in the table or an error occurred while the data set was being processed. In the latter case, a message (either ICH500I, ICH503I, ICH506I, ICH507I, ICH510I, or ICH515I) precedes this message.

System action: The system waits for the operator’s reply.

Operator response: Specify either the name of an alternate RACF database or NONE if no primary (or backup) RACF database is to be used for this sequence number.

Notes:
1. If an alternate database is specified, it must be online and cataloged.
2. If there is a problem with the primary RACF database, and RACF issues message ICH510I and ICH502A, you might (appropriately) reply to ICH502A with the name of the backup RACF database. RACF attempts to allocate the backup database as the primary database. If, following specifications in the data set name table, RACF then attempts to allocate the backup RACF database as the backup database, RACF will issue message ICH515I, then ICH502A again. This is normal, and you should consult with your system programmer about whether to reply with NONE or the name of yet another RACF database.

Programmer response: See “Problem Determination.”

Problem Determination: Be sure the RACF database is cataloged and online, and that the device on which the RACF database is mounted is functioning properly. If the database was updated by the IRRMIN00 utility, ensure that templates of the correct level were added to the RACF database. (Down-level templates can cause a RACF manager error.)

The data set name table (ICHRDSNT) should reside in SYS1.LINKLIB or any other APF-authorized linklist library. Make sure that you verify that the data set containing the ICHRDSNT is correctly APF authorized.

Destination: Descriptor code is 2. Routing code is 1.

ICH503I RACF DATA SET NOT FOUND [[PRIMARY | BACKUP] RACF DATA SET SEQUENCE nnn, dsname]
Explanation: During initialization, or the processing of a propagated RVARY ACTIVE command, the RACF database cannot be found.

System action: The system issues ICH502A following this message, then waits for the operator reply. If the system is enabled for sysplex communication and it is not the first system to IPL, message ICH502A is not issued and processing continues.

Operator response: Notify your system programmer.

Programmer response: Ensure that the correct RACF database is specified in MSTRJCL or that it is included in the operator’s reply to message ICH502A. Ensure that it is cataloged and online.

System programmer response: If this message is received during the processing of a propagated RVARY ACTIVE command on a SYSPLEX, (DATASHARING or SYSPLEX COMMUNICATION), and is followed by messages ICH529I and ICH532I, verify that the RACF DS named in ICH503I is cataloged on the same volume as the RACF DS of the same name on the member of the SYSPLEX on which the RACF RVARY ACTIVE command was entered. If the volume ids are not the same, recatalog the RACF DS to be on the same volume as the system on which the RVARY command was entered.

Destination: Descriptor code is 4. Routing code is 2.

ICH504I USER ATTRIBUTE DATA SET NOT FOUND

Explanation: During RACF initialization, the TSO UADS data set cannot be found. The UADS data set had been defined in MSTRJCL.

System action: The system continues with the IPL, but TSO/E is not usable until the next IPL.

Operator response: Report this message to the system programmer.

Programmer response: If you want to use TSO/E before the next scheduled IPL, you need to manually re-IPL the system to activate TSO/E.

Problem Determination: Ensure that the TSO UADS data set is cataloged and online.

Destination: Descriptor code is 4. Routing code is 2.

ICH505A RACF INITIALIZATION ABEND 'xxx' [ REASON CODE xxxxxxxx ]

Explanation: A system abend occurred during RACF initialization. Message ICH501I follows this message.

System action: IPL continues.

Operator response: Notify your system programmer.

Programmer response: See “Problem Determination.”

Problem Determination: See Chapter 11, “RACF” for system completion code xxx. The SDUMP data set and LOGREC data provide other diagnostic information. Correct the error and IPL again.

Destination: Descriptor codes are 1 and 2. Routing code is 1.

ICH506I RACF DATA SET CANNOT BE USED [[ PRIMARY | BACKUP ] RACF DATA SET SEQUENCE nnn, dsname]

Explanation: The data set is not usable as a RACF database for one of the following reasons:

1. The ICB indicates that the data set has been extended.
2. The data set was used as input in the IRRUT400 utility with the LOCKINPUT parameter specified.
3. The initialization of the RACF database failed.

Note: If this message is issued with either message ICH560I or ICH561I, see the information for those messages.

System action: The system issues ICH502A following this message, then waits for the operator’s reply.

Operator response: Notify your system programmer.

Programmer response: Ensure that the correct RACF database is specified in MSTRJCL or that it is included in the operator’s reply to message ICH502A.

Destination: Descriptor code is 4. Routing code is 2.

ICH507I RACF DATA SET NOT AT CURRENT RELEASE LEVEL [[ PRIMARY | BACKUP ] RACF DATA SET SEQUENCE nnn, dsname]

Explanation: The primary or backup RACF database being used is not at the appropriate release level.

System action: The system issues ICH502A following this message, then waits for the operator’s reply.

Operator response: Check the response to message ICH502A. It should be the name of a RACF database at the current release level. If this message recurs, report this message (and the response to message ICH502A) to the system programmer.

Programmer response: See “Problem Determination” for message ICH502A.

Destination: Descriptor code is 4. Routing code is 2.

ICH508I ACTIVE RACF EXITS: [NONE | name,...,name]

Explanation: During RACF initialization, one or more of the following installation exit routines or tables indicated by name were loaded from LPA and are in effect for this IPL:
ICH509I  •  ICH510I

ICH509I  SYSRACF DD STATEMENT NOT SPECIFIED IN MSTRJCL OR ALLOCATION FAILURE FOR RACF DATA SET.

Explanation: One of the following conditions occurred:

- RACF cannot find SYSRACF (a DD statement) in MSTRJCL.
- RACF cannot find the RACF database in the data set name table (ICHРDSNT).
- Dynamic allocation cannot allocate the RACF database. SYSRACF might be in the MSTRJCL but the RACF data set might not be cataloged in the correct volume.

System action: The system issues ICH502A following this message, then waits for the operator's reply. If the system is enabled for sysplex communication and it is not the first system to IPL, message ICH502A is not issued and processing continues.

Operator response: Notify your system programmer.

Programmer response: See “Problem Determination.”

Problem Determination: If SYSRACF has been removed from the MSTRJCL, check to see if the RACF database has been placed in the data set name table (ICHРDSNT). If not, correct the error and IPL again.

If the SYSRACF DD statement is present in MSTRJCL, the RACF database has been cataloged in the wrong volume. Catalog SYSRACF and IPL again.

The data set name table (ICHРDSNT) should reside in SYS1.LINKLIB or any other APF-authorized linklist library. Make sure that you verify that the data set containing the ICHРDSNT is correctly APF authorized.

Destination: Descriptor code is 4. Routing code is 2.

ICH510I  ALLOCATION FAILED FOR RACF DATA SET [[PRIMARY | BACKUP] RACF DATA SET SEQUENCE nnn, dsname]

Explanation: The attempt to dynamically allocate the database specified has failed.

System action: If this message is received during RACF initialization, it is followed by message ICH502A to prompt the operator for another data set name for the data set sequence number nnn. If the system is enabled for sysplex communication and it is not the
ICH511I • ICH512I

first system to IPL, message ICH502A is not issued and processing continues.

If this message is received during an RVARY request, message ICH502A is not issued and the RVARY command retries the activation of the data set.

**Operator response:** Notify the system programmer.

**System programmer response:** If this message is received during RACF initialization, verify that the name specified is a valid RACF data set name. If the specified name is correct, make sure that the device containing the data set is on line and available. Instruct the operator to reply to message ICH502A with the correct RACF data set name. If the specified name is incorrect, provide the operator with the correct RACF data set name for the data set sequence number nnn. The operator uses this name to reply to message ICH502A. Correct any errors in the data set name table.

If this message is received during the initialization of RACF on a system attempting to join a SYSPLEX, (DATASHARING or SYSPLEX COMMUNICATION), and is followed by message ICH510I, verify that the RACF DS named in ICH510I is cataloged on the same volume as the RACF DS of the same name on the current members of the SYSPLEX. If the volume ids are not the same, recatalog the RACF DS to be on the same volume as the current members of the SYSPLEX.

If this message is received during an RVARY request, make sure that the specified RACF data set is cataloged and the device containing the data set is on line and available. Reissue the RVARY command.

**Destination:** Descriptor code is 4. Routing code is 2.

| ICH511I | RACF DETECTED AN ERROR IN THE [IBM SUPPLIED | INSTALLATION] CLASS DESCRIPTOR TABLE, ENTRY entry-name, ERROR CODE yy |
|---------|---------------------------------------------------------------------------------------------------------------|

**Explanation:** RACF encountered an error for entry entry-name in either the installation-defined class descriptor table, ICHRRCDE, or the class descriptor table supplied by IBM, ICHRRCDX. The class descriptor table is located in one of the following locations:

- SYS1.LINKLIB
- A library concatenated to SYS1.LINKLIB
- LPA (for ICHRRCDE only)

This message is followed by message ICH501I. Error code yy identifies the problem as follows:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description of Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The class name is missing, contains embedded blanks or incorrect characters.</td>
</tr>
<tr>
<td>2</td>
<td>The ID field has a value of zero.</td>
</tr>
<tr>
<td>3</td>
<td>The POSIT mask has more than 1 bit turned on or has no bits turned on.</td>
</tr>
<tr>
<td>4</td>
<td>The field that defines the length of the class name (MAXLNTH or MAXLENX) is incorrect. The valid range is 1 to 246.</td>
</tr>
<tr>
<td>5</td>
<td>The class is designated as a resource group class, but the MEMBER field does not contain a member class name.</td>
</tr>
<tr>
<td>6</td>
<td>The table contains more than 1024 entries.</td>
</tr>
<tr>
<td>7</td>
<td>Two entries have the same class names.</td>
</tr>
<tr>
<td>8</td>
<td>One of the following conditions is true:</td>
</tr>
<tr>
<td></td>
<td>• A grouped class specifies a member that does not exist in the table or is incorrect, or a member class specifies a group that does not exist in the table or is incorrect.</td>
</tr>
<tr>
<td></td>
<td>• A pair of classes reference each other, but one or both is not a grouping class.</td>
</tr>
<tr>
<td>9</td>
<td>One of the reserved class names (USER, GROUP, or DATASET) appears in the class table.</td>
</tr>
<tr>
<td>10</td>
<td>An entry in the installation table has a class name with the same name as an entry in the table supplied by IBM.</td>
</tr>
<tr>
<td>11</td>
<td>The area reserved for the pointer to the RACLISTed profiles is not zero.</td>
</tr>
<tr>
<td>12</td>
<td>The area reserved for the pointer to the GENLISTed profiles is not zero.</td>
</tr>
<tr>
<td>13</td>
<td>The length of the class descriptor (CDT) entry (as indicated in a field in the entry itself) is not the same as the actual length of the class descriptor table entry.</td>
</tr>
</tbody>
</table>

**System action:** IPL continues.

**Operator response:** Ensure that the system parameters MLPA and LNK have been specified properly. If they are not, correct any errors and IPL again. Otherwise, notify your system programmer.

**Programmer response:** Ensure that no errors occurred during the assembly of the table entries, that the table was properly link-edited, and that modifications subsequent to link-edit did not cause an error. Correct the error and IPL again.

**Destination:** Descriptor code is 4. Routing code is 2.

<table>
<thead>
<tr>
<th>ICH512I</th>
<th>RACF UNABLE TO LOCATE modname IN LPA</th>
</tr>
</thead>
</table>

**Explanation:** RACF encountered one of the following errors:

- RACF searched the link-pack area and cannot locate one of the routines necessary for RACF processing. Processing cannot continue. Message ICH501I follows this message.
- RACF cannot locate ICHRFR00 in the link-pack area. Processing continues, but the user cannot invoke RACF with the RACROUTE macro instruction.
**ICH513I**  
Data set not referenced in range table primary RACF data set sequence \( mnn \), \( dsname \)  

**Explanation:** There are no entries in the range table that would allow access to the database indicated by \( dsname \) with sequence number \( mnn \).  

**System action:** The database is not available to RACF.  
**Operator response:** Notify your system programmer.  
**System programmer response:** Check for a mismatch between the data set name table (ICHRDSNT) and the range table (ICHRRNG).  
**Destination:** Descriptor code is 4. Routing code is 2.

**ICH517I**  
Error in range table.  

**Explanation:** Either the operator entered the incorrect MLPA or LNK value, or an entry in the range table is out of order. Message ICH501I follows this message.  

**System action:** IPL continues.  
**Operator response:** If the MLPA or LNK value was incorrect, correct it and IPL again. Otherwise, notify your system programmer of the error.  
**Programmer response:** Ensure that the range table (ICHRRNG) was assembled and link-edited correctly. If necessary, correct the order of the entries in the range table. IPL again.  
**Problem Determination:** The range table must contain at least one entry. The first entry must have a key of 44 binary zeros, and the entries must appear with their keys in ascending order.  
**Destination:** Descriptor code is 4. Routing code is 2.

**ICH518I**  
Error in initializing RACF data set.  

**Explanation:** RACF unsuccessfully defined the user profile or groups to a new RACF database. Message ICH501I follows this message.  

**System action:** IPL continues.  
**Operator response:** Notify your system programmer.  
**Programmer response:** See “Problem Determination.”  
**Problem Determination:** Ensure that the data set name table (ICHRDSNT) does not contain two entries with the same database name. Also, ensure that the operator does not respond to message ICH502A with the name of a database that already exists in the data set name table.  
**Destination:** Descriptor code is 4. Routing code is 2.
important. There should be a user profile (IBMUSER) and a group profile (SYS1) with IBMUSER connected to it.

**Destination:** Descriptor code is 4. Routing code is 2.

**ICH519I**  ERROR DURING UNALLOCATION OF RACF DATA SET.

**Explanation:** There was an error during an attempt to allocate a RACF resource because RACF cannot dynamically deallocate a database specified in the data set name table (ICHRDSNT) or specified in a response to the operator. Message ICH501I follows this message.

**System action:** IPL continues.

**Operator response:** Notify your system programmer.

**Programmer response:** Ensure that the databases actually exist and that they reside on the DASD volume that is specified in the catalog entry of the data set. Correct the error and IPL again.

**Destination:** Descriptor code is 4. Routing code is 2.

**ICH520I**  z/OS Security Server (RACF xxxxxxx) is active.

**Explanation:** RACF FMID xxxxx has been successfully initialized.

**System action:** IPL continues with RACF active.

**Destination:** Descriptor code is 4. Routing code is 2.

**ICH521I**  GLOBAL ACCESS CHECKING BASE TABLE NOT OBTAINED, NO STORAGE AVAILABLE.

**Explanation:** The attempt to obtain storage from subpool 241 for the global-profile-base-name table failed.

**System action:** RACF initialization continues, but global access checking is disabled.

**Operator response:** Notify the RACF security administrator and the system programmer.

**Programmer response:** Check the amount of storage available for use with subpool 241 and, if necessary, increase the amount of CSA available.

**Destination:** Descriptor code is 4. Routing code is 2.

**ICH522I**  ERROR IN STARTED PROCEDURES TABLE

**Explanation:** In the started procedures table, RACF found either a generic entry that was not the last entry or a generic entry that contains ‘=’ in both the user ID and group name fields.

**System action:** RACF initialization continues, but the generic entry is ignored.

**Operator response:** Notify your system programmer.

**Programmer response:** Correct the started procedures table, and if necessary, IPL again.

**Destination:** Descriptor code is 4. Routing code is 2.

**ICH523I**  ERROR DURING SVC TABLE UPDATE

**Explanation:** RACF encountered an error while trying to update the SVC table with the RACF SVC entry points. Message ICH501I follows this message.

**System action:** A system dump is produced. IPL continues.

**Operator response:** Notify your system programmer.

**Programmer response:** Determine the cause of the error and correct it.

**Destination:** Descriptor code is 4. Routing code is 2.

**ICH524I**  INSTALLATION CLASS DESCRIPTOR TABLE PROCESSED

**Explanation:** During RACF initialization, the installation-supplied class descriptor table was located in SYS1.LINKLIB, a library concatenated to SYS1.LINKLIB, or LPA. That table is in effect for this IPL.

**System action:** RACF initialization continues.

**Destination:** Descriptor code is 4. Routing code is 2.

**ICH525I**  INSTALLATION ROUTER TABLE PROCESSED

**Explanation:** During RACF initialization, the installation-supplied router table was located in SYS1.LINKLIB, a library concatenated to the SYS1.LINKLIB, or LPA. The table is in effect for this IPL.

**System action:** RACF initialization continues.

**Destination:** Descriptor code is 4. Routing code is 2.

**ICH526I**  RACF UNABLE TO LOCATE modname

**Explanation:** RACF encountered one of the following errors:

- RACF failed to locate the class descriptor table (ICHRRCDX) required for RACF processing. This table should be located in SYS1.LINKLIB or in a library concatenated to SYS1.LINKLIB. Processing cannot continue. Message ICH501I follows this message.
- RACF cannot locate the MVS router table (ICHRFR0X). This table should be located in SYS1.LINKLIB or in a library concatenated to SYS1.LINKLIB. Processing continues, but the user cannot invoke RACF with the RACROUTE macro instruction.

**System action:** RACF initialization continues, but the generic entry is ignored.
ICH527I  RACF DETECTED AN ERROR IN THE INSTALLATION ROUTER TABLE,
ENTRY entry-name, ERROR CODE yy

Explanation:  RACF locates the installation-defined RACF router table, ICHRFR01 in one of the following:
• SYS1.LINKLIB
• A library concatenated to SYS1.LINKLIB
• LPA

RACF ensures that each class name satisfies certain conditions. RACF issues this message to the operator when the table contains an error.

System action:  RACF uses the first entry name and ignores additional duplicate name(s).

Operator response:  Check for errors in the specification of the system parameters MLPA and LNK. If there are errors, correct them and IPL again. If there are no errors, report the exact text of this message to your system programmer.

System programmer response:  Ensure that no errors occurred during the assembly of the table entries, that the table was properly link-edited, and that modification subsequent to link-edit did not cause the error. Correct the error and IPL again.

Problem Determination:  The error code yy identifies the problem as follows:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description of Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An entry in the installation-supplied portion of the router table duplicates the class name, requester, and subsystem ID of an entry in the portion of the table supplied by IBM.</td>
</tr>
</tbody>
</table>

Note:  Error code 1 is no longer issued as of z/OS Version 1 Release 6 since ICHRFR0X has been removed.

| 2    | An entry in the installation-supplied portion of the router table has the class name specified in another installation-supplied entry. |

Destination:  Descriptor code is 4. Routing code is 2.

ICH529I  RVARY ALLOCATION/DEALLOCATION FAILED

Explanation:  An RVARY command was issued, and the allocation or deallocation of the RACF database failed.

User response:  Check that the data set name specified on the RVARY command is correctly spelled. If the data set name is spelled correctly, contact the system programmer.

System programmer response:  Check that the data set specified on the RVARY command actually exists. If the data set specified on the RVARY command exists, check the DASD for problems.

Destination:  Descriptor code is 4. Routing code are 2 and 11.

ICH530I  I/O ERROR DURING DATASET ALLOCATION/DEALLOCATION
[[PRIMARY | BACKUP] RACF DATA SET SEQUENCE nnn, dsname]

Explanation:  An I/O error occurred during the allocation or deallocation of the RACF database.

System action:  The system issues message ICH502A to prompt for a new data set name.

System programmer response:  If necessary, switch to a backup RACF database (using the RVARY SWITCH command).

Note:  For complete information about recovering from the problem, see the section on RACF database recovery in z/OS Security Server RACF System Programmer's Guide. Pay particular attention to the section on failures during I/O operations on the RACF database in z/OS Security Server RACF System Programmer's Guide.

Problem Determination:  Other messages might have been issued for this problem. These messages might display on the system console or the security console, or end users might receive them. An analysis of those messages might help you determine the cause of the problem. In particular, look for message ICH51011I, that reports a return code from the RACF manager.

Destination:  Descriptor code is 4. Routing code are 2 and 11.
ICH531I  RACF DATA SET ALLOCATION/DEALLOCATION INTERFACE IS ACTIVE.
Explanation: The facility that permits the RACF database to be allocated or deallocated automatically when the RVARY command is issued is active.
Destination: Descriptor code is 4. Routing code is 2.

ICH532I  RVARY REQUEST TERMINATED DUE TO ERROR.
Explanation: An error occurred during RVARY processing.
System action: RACF stops processing the command and issues message ICH5009I to the issuer of the RVARY command.
Operator response: Report this message to the system programmer.
Programmer response: IPL again and reissue the RVARY command.
Problem Determination: If this message recurs, call your IBM support center.
Destination: Descriptor code is 4. Routing codes are 2 and 11.

ICH533I  CLASS class-name IS ACTIVE, BUT RACLIST FOR THE CLASS FAILED. RACLIST MACRO RETURN CODE IS return-code.
Explanation: At IPL, RACROUTE REQUEST=LIST processing cannot be performed for the indicated class.
System action: No in-storage profiles are created for the indicated class. RACF still protects the same resources, but system performance might be adversely affected.
Operator response: Report the exact text of this message to your system programmer.
System programmer response: Check with the RACF security administrator to see if this condition will cause a performance problem on the system. If so, re-IPL the system.
Problem Determination: See z/OS Security Server RACROUTE Macro Reference for the indicated return and reason codes from the REQUEST=LIST macro.
Destination: Descriptor code is 4. Routing codes are 2 and 11.

ICH534I  CLASS class-name IS ACTIVE, BUT RACLIST FOR THE CLASS FAILED. RACLIST MACRO RETURN CODE IS return-code. REASON CODE IS reason-code.
Explanation: At IPL, RACROUTE REQUEST=LIST processing cannot be performed for the indicated class.
System action: No in-storage profiles are created for the indicated class. RACF still protects the same resources, but system performance might be adversely affected.
Operator response: Report the exact text of this message to your system programmer.
System programmer response: Check with the RACF security administrator to see if this condition will cause a performance problem on the system. If so, re-IPL the system.
Problem Determination: See z/OS Security Server RACROUTE Macro Reference for the indicated return and reason codes from the REQUEST=LIST macro.
Destination: Descriptor code is 4. Routing codes are 2 and 11.

ICH537I  RACF IS NOT ACTIVE. RACF IS UNABLE TO LOAD MANAGER xxxxxxxx.
Explanation: The RACF manager that is identified in the message cannot be loaded from SYS1.LINKLIB. Message ICH501I follows this message.
System action: RACF is not activated.
Operator response: Contact the system programmer.
System programmer response: Check the RACF installation procedure to determine the reason the RACF manager's load module is missing from the load library. Ensure that the manager's load module is present on the load library before attempting to activate RACF.
ICH538I  RACF MESSAGE TASK ABEND $xxx.

Explanation: An ABEND occurred during RACF message subtask processing.

System action: RACF remains active and the message subtask will attempt to restart.

Operator response: Notify the system programmer.

Programmer response: See “Problem Determination.”

Problem Determination: See your MVS system codes documentation for completion code $xxx. The SDUMP data set and LOGREC data provide other diagnostic information.

Destination: Descriptor code is 4. Routing code is 2.

ICH539I  UNABLE TO ESTABLISH RECOVERY ENVIRONMENT, RACF MESSAGE TASK TERMINATED.

Explanation: The RACF message subtask got a nonzero return code from an ESTAE macro instruction.

System action: The message subtask stops. RACF remains active but RACF SRB mode services are unable to issue messages.

Operator response: Notify the system programmer.

Programmer response: See “Problem Determination.”

Problem Determination: For a description of the ESTAE return code, see z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG.

Destination: Descriptor code is 4. Routing codes are 2 and 11.

ICH540I  RACF MESSAGE TASK TERMINATED.

Explanation: Either four recursive abends (no requests successfully processed between abends) or a total of eleven abends have occurred during RACF message subtask processing.

System action: The message subtask stops. RACF remains active but RACF SRB mode services are unable to issue messages.

Operator response: Notify the system programmer.

Programmer response: See “Problem Determination.”

Problem Determination: See your MVS system codes documentation for completion code $xxx. The SDUMP data set and LOGREC data provide other diagnostic information.

Destination: Descriptor code is 4. Routing code is 2.

ICH541I  RACINIT {CREATE | DELETE} FAILED.

RETURN CODE IS return-code.

Explanation: At IPL, during RACROUTE REQUEST=LIST processing, the creation or deletion of an ACEE by way of REQUEST=VERIFY failed. The message is issued to both the operator and the security console.

System action:
- If this occurred during creation of the ACEE, no in-storage profiles are created for any class. RACF still protects the same resources, but system performance might be adversely affected.
- If this occurred during deletion of the ACEE, in-storage profiles are created and system performance is not affected. However, storage is being wasted by the ACEE and should be deleted.

Operator response: Report the exact text of this message to your system programmer.

System programmer response: This condition can cause a performance problem on the system. For example, on CREATE, no REQUEST=LIST processing takes place. This can cause performance degradation. If so, re-IPL the system. On DELETE, performance is not adversely affected; however, storage is being wasted by the ACEE (or ACEEs) that have not been deleted. If the problem persists, contact IBM.

Problem Determination: See z/OS Security Server RACROUTE Macro Reference for the indicated return and reason codes from the REQUEST=VERIFY macro.

Destination: Descriptor code is 4. Routing codes are 2 and 11.

ICH542I  RETURN CODE FROM RACROUTE MACRO IS return-code.

Explanation: At IPL, during RACROUTE REQUEST=LIST processing, the REQUEST=LIST and REQUEST=VERIFY macros are invoked by RACROUTE. If one fails, RACROUTE returns its own return code and the return and reason codes of the called macros. For example, if the RACROUTE return code is 4, and a called REQUEST=LIST return and reason codes are 0, this means that the class is not in the router table and the REQUEST=LIST processing was not done. The message is issued to both the operator and the security console when, for example, there is an error creating an ACEE during REQUEST=LIST processing.

System action: No in-storage profiles are created for the indicated class. RACF still protects the same resources, but system performance might be adversely affected.

Operator response: Report the exact text of this message to your system programmer.

System programmer response: This condition can cause a performance problem on the system. For example, on CREATE, no REQUEST=LIST processing takes place. This can cause performance degradation. If so, re-IPL the system.

Problem Determination: See z/OS Security Server RACROUTE Macro Reference for the indicated return
and reason codes from the RACROUTE macro.

**Destination:** Descriptor code is 4. Routing codes are 2 and 11.

**ICH544I** RACLIST DID NOT OCCUR FOR ANY OF THE RACF CLASSES CONTACT YOUR SYSTEM ADMINISTRATOR.

**Explanation:** During IPL, RACF initialization was not able to create an ACEE needed for RACROUTE REQUEST=LIST processing. As a result none of the RACF classes can be RACLISTed. This message is issued to both the operator and the security console.

**System action:** For classes that are not part of a grouping member class pair and defined with RACLREQ=NO (REQUEST=LIST not required), normal authorization checking occurs, although system performance may be adversely affected.

For classes that are part of a grouping member class pair and defined with RACLREQ=NO (REQUEST=LIST not required), authorization checking experiences performance problems. In addition, authorization checking may be wrong, because only the profiles in the member class are considered when making decisions. The profiles in the grouping class are ignored, because they are used only when the RACLIST is successful.

For classes defined with RACLREQ=YES (REQUEST=LIST is required), ALL authorization requests for the class will result in return code 4.

**Operator response:** Report the exact text of this message to your system programmer.

**System programmer response:** This condition can cause other components and applications to fail because of RACROUTE REQUEST=AUTH return code 4 for RACLREQ=NO classes. In addition, this condition can cause performance degradation. If either of these problems occur, re-IPL Message ICH544I follows this message and indicates the cause of the error.

**Destination:** Descriptor code is 4. Routing codes are 2 and 11.

**ICH545I** WARNING: THE RACF DATA SET JUST ACTIVATED IS LOCKED. (PRIMARY | BACKUP) DATA SET SEQUENCE nnn, dsname

**Explanation:** During RVARY command processing, RACF detected that data set dsname is locked. This data set is a primary or backup data set for the sequence number indicated by nnn.

**System action:** The RVARY ACTIVE command completes successfully. Data set dsname remains locked.

**Operator response:** Report this message to your system programmer.

**ICH546I** CLASS classname IS ACTIVE, BUT RACLIST FOR THE CLASS FAILED. DATA SPACE FAILURE RETURN CODE IS return-code, REASON CODE IS reason-code.

**Explanation:** At IPL, RACLIST processing cannot be performed for the indicated class because of a problem in processing data spaces. The return and reason codes can help the IBM support center determine the cause of the problem.

**System action:** For classes that are not part of a grouping member class pair, no in-storage profiles are created for the indicated class. In addition to issuing this message, the system may have taken an SVC dump. RACF still protects the same resources, but system performance may be adversely affected.

For classes that are part of a grouping member class pair, authorization checking experiences performance problems. In addition, authorization checking may be wrong, because only the profiles in the member class are considered when making decisions. The profiles in the grouping class are ignored, because they are used only when the RACLIST is successful.

For the CDT class, the dynamic class descriptor table is not built. No dynamic classes are available for RACF processing.

**Operator response:** Report the exact text of this message to your system programmer.

**System programmer response:** Have the RACF security administrator issue SETROPTS RACLIST(classname). If this command fails with messages ICH14031I and ICH14058I, proceed to problem determination.

**Problem Determination:** Call your IBM support center. Have the message text available and the SVC dump, if one was taken. The return code and reason code values in the message are:

<table>
<thead>
<tr>
<th>Return code</th>
<th>Reason code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>04</td>
<td>04</td>
<td>ALESERV ADD function failed</td>
</tr>
<tr>
<td>08</td>
<td>04</td>
<td>TCBTOKEN function failed</td>
</tr>
<tr>
<td>08</td>
<td>04</td>
<td>DSPSERV CREATE function failed</td>
</tr>
<tr>
<td>12</td>
<td>04</td>
<td>ALESERV ADD function failed</td>
</tr>
</tbody>
</table>
ICH549I  RACF DATABASE dbname DOES NOT RESIDE ON SHARED DASD.

**Explanation:** If RACF sysplex communication is wanted, the RACF database must be on a shared DASD. If sysplex communication is not wanted, you must turn off the data sharing bit in the data set name table (ICHRDSNT). See the MVS documentation on planning I/O configurations. This message may also be issued if RACF is installed for data sharing and an RVARY command was issued in an attempt to activate a data set that does not reside on a shared DASD. In this case, the data set will simply not be activated. Message ICH501I follows this message.

**System action:** RACF enters failsoft processing.

**System programmer response:** If sysplex communication is wanted, ensure the RACF database is on a shared device. Verify that the data set name table (ICHRDSNT) is accurate and re-IPL. If sysplex communication is not wanted, correct the bit setting in ICHRDSNT and re-IPL.

**Destination:** Descriptor code is 4. Routing code is 2.

ICH550I  SYSTEM sysname IS IN LOCAL SYSPLEX MODE. IT CANNOT BE ENABLED FOR SYSPLEX COMMUNICATION.

**Explanation:** Either the sysplex communication bit or the default mode bit in the data set name table (ICHRDSNT) is on, but the system is in local sysplex mode. In order for RACF to be enabled for sysplex communication, the system must be in non-local sysplex mode. RACF enters failsoft mode on this system. Message ICH501I follows this message.

**System action:** RACF continues initialization in failsoft processing.

**System programmer response:** If sysplex communication is wanted, change the system to run in non-local sysplex mode and re-IPL. See the MVS documentation on planning sysplex management to determine the problem. If sysplex communication is not wanted, ensure that the sysplex communication bit and the default mode bit are off in ICHRDSNT and re-IPL.

**Destination:** Descriptor code is 4. Routing code is 2.

ICH551I  DATA SHARING WAS REQUESTED, HOWEVER SYSTEM sysname IS NOT RUNNING ON THE MINIMUM MVS RELEASE LEVEL REQUIRED.

**Explanation:** The indicated system is installed for data sharing but is not running on the minimum MVS release level required. Message ICH501I follows this message.

**System action:** RACF continues initialization in failsoft processing.

**System programmer response:** Notify the system programmer.

**System action:** RACF will enter failsoft processing.

**System programmer response:** Notify your system programmer.

**System action:** RACF enters failsoft processing.

**System programmer response:** For documentation on the IXCJOIN return and reason codes, see the appropriate MVS documentation. If necessary, report the problem to the appropriate IBM support center.

**Destination:** Descriptor code is 4. Routing code is 2.
ICH554I • ICH556I

ICH554I  NUMBER OF RESIDENT DATA BLOCKS SPECIFIED IN ICHRDSNT FOR DATABASE dbname IS INSUFFICIENT FOR SYSPLEX COMMUNICATION. DEFAULT OF 50 FOR PRIMARY AND 10 FOR BACKUP WILL BE USED.

Explanation:  When installed for sysplex communication, RACF requires a minimum of 50 resident data blocks for the primary and a minimum of 10 resident data blocks for the backup. The number of resident data blocks specified for the primary is less than 50 for the indicated database.

System action:  RACF allocates a default of 50 resident data blocks for the primary and 10 resident data blocks for the backup for this IPL and continues initialization.

Operator response:  Notify the system programmer.

System programmer response:  Update the data set name table (ICHRDSNT) to specify at least 50 resident data blocks for the indicated database before the next IPL.

Destination:  Descriptor code is 4. Routing code is 2.

ICH555I  table_name FOR MEMBER memname DOES NOT MATCH table_name FOR IRRXCF00 GROUP. GROUP table_name IS USED.

Explanation:  There is an inconsistency between the table defined for member memname, and the in-storage table established for the data sharing group, IRRXCF00. RACF uses the table established for the data sharing group.

- If the table name is ICHRDSNT, the data set names or flag settings in the table defined for member memname do not match those in use by the other members of the data sharing group.
- If the table name is ICHRRNG, the contents of the range table for member memname do not match those in use by the other members of the data sharing group.

System action:  RACF continues initialization using the table established for the data sharing group, IRRXCF00.

Operator response:  Contact your system programmer.

System programmer response:  Correct the inconsistency in the table for member memname to avoid this message during the next IPL. If the table name is ICHRDSNT and the table for member memname in this message has been verified, issue an RVARY LIST command on the logical partition where this message occurs and check for differences between the data set table name (ICHRDSNT) and the information returned from the RVARY LIST command. For example, you can check the primary and backup database and determine if they are the same. See z/OS Security Server RACF System Programmer's Guide for more information.

Destination:  Descriptor code is 4. Routing code is 2.

ICH556I  RACF MANAGER INVOCATION FOR RVARY ENDED DUE TO ERROR. RETURN CODE = X'nnnnnnnn'.

Explanation:  This message is the result of a failure during the propagation of an RVARY request to members of the RACF data sharing group. This error was encountered during an attempt to refresh RACF control information from a newly activated master data set. The refresh may not have been completed.

The RACF manager cannot complete the requested operation because of a system error or a problem with the RACF database. The return code is a RACF manager return code that is not recognized by the command processor that invoked the RACF manager.

System action:  Command processing completes, but RACF system options may not have been refreshed.

Operator response:  Report this message to your system programmer.

System programmer response:  Determine the RACF manager problem. After the problem has been corrected, RVARY INACTIVE and RVARY ACTIVE can be issued against the master data set to ensure that RACF control information has been correctly refreshed.

Problem Determination:  If there is an error in the RACF database, the RACF manager issues message ICH411I preceding this message. See this message for information about how to resolve the problem.

Note:  If the user is not receiving write-to-programmer messages, message ICH411I is not received. To receive this message, issue the TSO/E command PROFILE WTPMSG MSGID and rerun the RACF command or utility.

Check the list of RACF manager return codes in "RACF manager return codes" on page 405. If the return code is listed, the explanation should help you investigate the problem. If the return code is not listed or relates to a problem with RACF (as opposed to a problem you can fix in the RACF database), report the complete text of this message to your IBM support center.

For certain return codes, this message might be issued because there is a bad profile in the RACF database. To find the bad profile, enter the SEARCH command. With a bad profile in the database, this command is likely to fail also. The profile after the last one listed is probably the bad profile. Because this command might take a long time to run and might produce many lines of output, you might want to run the command in batch mode.

Destination:  Descriptor code is 4. Routing code is 2.
ICH557I UNABLE TO ESTABLISH RECOVERY FOR PROPAGATED RVARY COMMAND.

Explanation: RACF attempted to process a propagated RVARY request on this member of a RACF data sharing group, but was unable to establish recovery.

System action: RACF did not process the command on this member.

Operator response: Report this message to your system programmer.

System programmer response: This might be an indication of additional system problems. Look for related messages in the system log. Correct these problems and try again. If the problem persists, call your IBM support center.

Destination: Descriptor code is 4. Routing code is 2.

ICH558I MEMBER memname IS NOT AT SUFFICIENT MVS LEVEL TO EXECUTE THIS RVARY COMMAND.

Explanation: All members of the RACF data sharing group must be at MVS 5.1 or above for an RVARY DATASHARE or RVARY NODATASHARE command to function. This message indicates that the member to which the command was issued was at the sufficient level but the member memname was not.

System action: RACF does not process the command.

Operator response: None.

System programmer response: If data sharing is wanted, all the members of the RACF data sharing group must be upgraded to MVS 5.1 or above.

Destination: Descriptor code is 4. Routing code is 2.

ICH559I MEMBER memname ENABLED FOR SYSPLEX COMMUNICATIONS.

Explanation: At this point in RACF initialization, the member memname is enabled for sysplex communications as requested by the installation in its data set name table (ICHRDSNT). This allows the member to participate in RVARY and SETROPTS command propagation. Additionally, if all systems in the RACF data sharing group are at MVS 5.1 or above and the installation has a coupling facility, the member can also participate in RACF data sharing.

System action: RACF initialization continues.

Operator response: None.

System programmer response: None.

Destination: Descriptor code is 4. Routing code is 2.

ICH560I COULD NOT CAPTURE UCB FOR RACF DATA SET. IOSCAPU FAILED WITH RETURN CODE X'return-code' AND REASON CODE X'reason-code'.

Explanation: In MVS 5.2.0 and later environments, RACF data sets can reside on devices whose UCB is above 16MB. RACF issued the IOSCAPU macro to “capture” the UCB into a window below 16MB, and the capture request failed.

System action: The system issues message ICH506I following this message.

If this message is received during RACF initialization, the system also issues message ICH502A following this message, which prompts the operator to enter a new data set name or ‘NONE’. The system then waits for the operator’s reply. Message ICH502A will not occur if this system is in data sharing mode and is not the first system in the sysplex.

If this message is received during an RVARY request, message ICH502A is not issued, and the RVARY command retries the activation of the data set five times.

Operator response: Notify your system programmer.

System programmer response: See the MVS documentation for the IOSCAPU return and reason codes to determine why the UCB for the device containing the RACF data set cannot be “captured” and correct the problem.

If this message was received during RACF initialization, the operator should be instructed to reply to message ICH502A with the same data set name after the problem has been corrected.

If this message was received during an RVARY request, the RVARY command should be reissued after the problem has been corrected.

ICH561I COULD NOT UNCAPTURE UCB FOR RACF DATA SET. IOSCAPU FAILED WITH RETURN CODE X'return-code' AND REASON CODE X'reason-code'.

Explanation: In MVS 5.2.0 and later environments, RACF data sets can reside on devices whose UCB is above 16MB. When a RACF data set is deactivated, RACF issues the IOSCAPU macro to “uncapture” a UCB that may have been “captured” into a window below 16MB when the data set was activated and the uncapture request failed.

System action: The system issues message ICH506I following this message. Deactivation of the RACF data set continues.

Operator response: Notify your system programmer.

System programmer response: See the MVS documentation for the IOSCAPU return and reason codes to determine why the UCB for the device...
containing the RACF data set cannot be “uncaptured”.

ICH562I  AN ATTEMPT TO CREATE A RACF RESOURCE MANAGER TO HANDLE ADDRESS SPACE TERMINATION HAS FAILED, AS INDICATED BY THE RESMGR SERVICE WITH RETURN CODE X’return-code’.

Explanation:  The MVS service for resource manager creation (RESMGR) failed with return code return-code.

System action:  RACF is initialized in read-only mode. For information about RACF sysplex data sharing modes, see z/OS Security Server RACF System Programmer’s Guide.

System programmer response:  Consult the MVS or z/OS documentation for information about RESMGR return codes and try to correct the problem.

• If you corrected the problem, issue the RVARY DATASHARE command.
• If you cannot correct the problem, report the exact text of this message to the appropriate IBM support center.

Destination:  Descriptor code is 4. Routing code is 2.

ICH564A  RACF DETECTED AN ERROR IN THE [IBM SUPPLIED | INSTALLATION] CLASS DESCRIPTOR TABLE, ENTRY entry-name, ERROR CODE yy

Explanation:  RACF encountered an error for entry entry-name, in either the installation-defined class descriptor table, ICHRRCDE, or the class descriptor table supplied by IBM, ICHRRCDX. The class descriptor table is located in one of the following locations:

• SYS1.LINKLIB
• A library concatenated to SYS1.LINKLIB
• LPA (for ICHRRCDE only)

This message is followed by message ICH501I. Error code yy identifies the problem as follows:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description of Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The class name is less than 4 characters or contains embedded blanks or non-alphanumeric characters.</td>
</tr>
<tr>
<td>2</td>
<td>The ID field has a value of zero.</td>
</tr>
<tr>
<td>3</td>
<td>The POSIT mask has more than 1 bit turned on or has no bits turned on.</td>
</tr>
<tr>
<td>4</td>
<td>The field that defines the length of the class name (MAXLTH or MAXLENX) has a value greater than 246.</td>
</tr>
<tr>
<td>5</td>
<td>The class is designated as a resource group class, but the MEMBER field does not contain a member class name.</td>
</tr>
<tr>
<td>6</td>
<td>The table contains more than 1024 entries.</td>
</tr>
<tr>
<td>7</td>
<td>Two entries have the same class names.</td>
</tr>
</tbody>
</table>
| 8    | One of the following conditions is true:  
• A grouped class specifies a member that does not exist in the table or is incorrect, or a member class specifies a group that does not exist in the table or is incorrect.  
• A pair of classes reference each other, but one or both is not a grouping class. |
| 9    | One of the reserved class names (USER, GROUP, or DATASET) appears in the class table. |
| 10   | An entry in the installation table has a class name with the same name as an entry in the table supplied by IBM. |
| 11   | The area reserved for the pointer to the RACLISTed profiles is not zero. |
| 12   | The area reserved for the pointer to the GENLISTed profiles is not zero. |
| 13   | The length of the class descriptor table entry (as indicated in a field in the entry itself) is not the same as the actual length of the class descriptor table entry. |

System action:  IPL continues.

Operator response:  Ensure that the system parameters MLPA and LNK have been specified properly. If they are not, correct any errors and IPL again. Otherwise, notify your system programmer.

Programmer response:  Ensure that no errors occurred during the assembly of the table entries, that the table was properly link-edited, and that modifications subsequent to link-edit did not cause an error. Correct the error and IPL again.

Destination:  Descriptor code is 2. Routing code is 1.

ICH565A  RACF UNABLE TO LOCATE modname IN LPA

Explanation:  RACF issues this message for two possible reasons:

• RACF searched the link-pack area and cannot locate one of the routines necessary for RACF processing. Processing cannot continue. Message ICH501I follows this message.
• RACF cannot locate ICHRFR00 in the link-pack area. Processing continues, but the user cannot invoke RACF with the RACROUTE macro instruction.

System action:  IPL continues.

Operator response:  Ensure that the system parameters MLPA and LNK have been specified properly. If they are not, correct any errors and IPL again. Otherwise, notify your system programmer.
Programmer response: If the system parameters MLPA and LNK have been properly specified, one of the following conditions has happened:

- RACF has not been installed properly.
- The MLPA and LNK lists do not contain all the entries necessary to load the RACF-required modules into the link-pack area.
- There is an error in the link-edit of a required routine.

Correct the error and IPL again.

Destination: Descriptor code is 2. Routing code is 1.

ICH566A  ERROR IN RANGE TABLE.

Explanation: Either the operator entered the incorrect MLPA or LNK value, or an entry in the range table is out of order. Message ICH501I follows this message.

System action: IPL continues.

Operator response: If the MLPA or LNK value was incorrect, correct it and IPL again. Otherwise, notify your system programmer of the error.

Programmer response: Ensure that the range table (ICHRRNG) was assembled and link-edited correctly. If necessary, correct the order of the entries in the range table. IPL again.

Problem Determination: The range table must contain at least one entry. The first entry must have a key of 44 binary zeros, and the entries must appear with their keys in ascending order.

Destination: Descriptor code is 2. Routing code is 1.

ICH567A  ERROR IN INITIALIZING RACF DATA SET.

Explanation: RACF cannot define the user profile or groups to a new RACF database. Message ICH501I follows this message.

System action: IPL continues.

Operator response: Notify your system programmer.

Programmer response: Reinitialize the new RACF databases and IPL again.

Problem Determination: The first time you IPL with RACF active, RACF generates a basic set of profiles. How these profiles are defined to each other is important. There should be a user profile (IBMUSER) and a group profile (SYS1) with IBMUSER connected to it.

Destination: Descriptor code is 2. Routing code is 1.
administrator and the system programmer.

**Problem Determination:** The SDUMP data set provides diagnostic information. Correct the error and IPL again.

**Destination:** Descriptor code is 2. Routing code is 1.

---

**ICH572A**  RACF IS NOT ACTIVE. RACF UNABLE TO LOAD MANAGER

**Explanation:** The RACF manager that is identified in the message cannot be loaded from SYS1.LINKLIB. Message ICH501I follows this message.

**System action:** RACF is not activated.

**Operator response:** Contact the system programmer.

**System programmer response:** Check the RACF installation procedure to determine the reason the RACF manager's load module is missing from the load library. Ensure that the manager's load module is present on the load library before attempting to activate RACF.

**Destination:** Descriptor code is 2. Routing code is 1.

---

**ICH573A**  RACF DATABASE dbname DOES NOT RESIDE ON SHARED DASD.

**Explanation:** The data set name table (ICHRDSNT) indicates that you want RACF sysplex communication, but RACF database dbname does not reside on the shared DASD.

This message can also be issued if RACF is installed for data sharing and the RVARY command was issued in an attempt to activate a data set that does not reside on a shared DASD. In this case, the data set is not activated. Message ICH501I follows this message.

**System action:** RACF enters failsoft processing.

**System programmer response:** Check the RACF installation procedure to determine the reason the RACF database dbname for sysplex communication is not present on the shared DASD. Ensure that the dbname is present on the shared DASD before attempting to activate RACF.

**Destination:** Descriptor code is 2. Routing code is 1.

---

**ICH574A**  SYSTEM sysname IS IN LOCAL SYSPLEX MODE. IT CANNOT BE ENABLED FOR SYSPLEX COMMUNICATION

**Explanation:** Either the sysplex communication bit or the default mode bit in the data set name table (ICHRDSNT) is on, but the system is in local sysplex mode. In order for RACF to be enabled for sysplex communication, the system must be in non-local sysplex mode. Message ICH501I follows this message.

**System action:** RACF enters failsoft processing.

**System programmer response:** If you want sysplex communication, change the system to run in non-local sysplex mode and IPL again. See the z/OS documentation on planning sysplex management to determine the problem. If you do not want sysplex communication, turn off the sysplex communication bit and the default mode bit in ICHRDSNT and IPL again.

**Destination:** Descriptor code is 2. Routing code is 1.

---

**ICH575A**  DATA SHARING WAS REQUESTED, HOWEVER SYSTEM sysname IS NOT RUNNING ON THE MINIMUM MVS RELEASE LEVEL REQUIRED.

**Explanation:** The indicated system is installed for data sharing but is not running on the minimum MVS release level required. Message ICH501I follows this message.

**System action:** RACF continues initialization in failsoft processing.

**Operator response:** Notify the system programmer.

**System programmer response:** If you want RACF sysplex data sharing, upgrade the system to at least MVS 5.1.0. If you do not want RACF sysplex data sharing, turn off the data sharing bit in the data set name table (ICHRDSNT) and IPL again.

**Destination:** Descriptor code is 2. Routing code is 1.

---

**ICH576A**  RACF ON SYSTEM sysname IS UNABLE TO JOIN GROUP IRRXCF00. IXCJOIN FAILED WITH RETURN CODE X’retcode’ AND REASON CODE X’rsncode’

**Explanation:** RACF attempted to join the RACF sysplex data sharing group, IRRXCF00, on system sysname. RACF experienced failures as shown in return code X’retcode’ and reason code X’rsncode’ for the IXCJOIN service. Message ICH501I follows this message.

**System action:** RACF enters failsoft processing.

**Operator response:** Notify your system programmer.

**System programmer response:** For documentation on the IXCJOIN return and reason codes, see the appropriate MVS documentation. If necessary, report the problem to the appropriate IBM support center.

**Destination:** Descriptor code is 2. Routing code is 1.
**ICH577E**  WARNING: segment-name SEGMENT OF template-type TEMPLATE AT LEVEL template-level DOES NOT CONTAIN FIELD field-name.

**Explanation:** RACF initialization has determined that a critical field is missing from the templates on the RACF database. This indicates that the level of the RACF initialization code is higher than the level of the templates on the RACF database. RACF initialization continues, but functions related to this field will not be available.

If the message indicates that the LDAPPROF field of the EIM (Enterprise Identity Mapping) segment in the USER template is missing, the following function is not available:

*Enterprise Identity Mapping*

If the message indicates that the ENCRYPT field of the KERB segment of the USER template is missing, then support for SETROPTS KERBLVL=1 and multiple key support for the KERB segment is unavailable, and a failure starting dynamic parse is also likely.

If the message indicates that the UNVFLG field of the BASE segment of the GROUP template is missing, then the ability to define groups with the universal group function is unavailable.

If the message indicates that the FLAG9 field of the BASE segment of the USER template type is missing, then the following functions are unavailable:

- Restricted access user ID functions
- Certificate name filter functions

If the message indicates that the KERBNAME field of the KERB segment of the USER template type is missing, then support for Network Authentication and Privacy Service is unavailable, and a failure starting dynamic parse is also likely.

If the message indicates that the ENCRYPT field of the KERB segment of the USER template is missing, then support for SETROPTS KERBLVL=1 and multiple key support for the KERB segment is unavailable, and a failure starting dynamic parse is also likely.

If the message indicates that the RACDHDR field of the BASE segment of the GENERAL template is missing, then a failure starting dynamic parse is likely and the following functions are unavailable:

- Support for hardening the cache to the RACF database as profiles in the CACHECLS class, or restoring the cache from those profiles, during the processing of an R_cacheserv callable service.
- RACF command support for User and General Resource profile PROXY segments.

Dynamic parse is required to parse segment-related keywords. It is used to add, list, alter, or delete DFP, TSO, or any other non-base segment information with the RACF commands. When dynamic parse fails to start, command processors that allow segment information will not work.

**System action:** IPL continues, but certain RACF functions may not be available.

**Operator response:** Notify your system programmer.

**System programmer response:** Run IRRMIN00 with PARM=UPDATE to update the templates to the correct level. Ensure that the correct RACF database has been specified. After you run IRRMIN00, you must re-IPL before the template changes become effective. If you are already using the function that is not available, you should re-IPL as soon as possible after you update the templates. If you are not currently using this function, you may re-IPL at any convenient time after you perform the update. The function remains unavailable until re-IPL.

**Destination:** Descriptor code is 11. Routing codes are 1, 9 and 10.

---

**ICH578I**  REQUEST FOR EIM REGISTRY FAILED. ICHEINTY RETURN CODE xxx AND REASON CODE xxx.

**Explanation:** An unexpected return code was received from ICHEINTY while attempting to retrieve the EIM RACF registry name.

**System action:** IPL continues. EIM applications using the default registry name will not function correctly.

**Operator response:** Report the exact text of this message to your system programmer.

**System programmer response:** Determine the cause of the error, correct it, and try again. If the problem persists, contact your RACF Security Administrator.

**Destination:** Descriptor code is 4. Routing codes are 2 and 11.

---

**ICH579E**  RACF TEMPLATES ON DATABASE ARE DOWNLEVEL: FMID or APAR rrrrrrrrr.aaaaaaaa USING TEMPLATES AT LEVEL FMID or APAR rrrrrrrrr.aaaaaaaa FROM IRRTEMP2. RUN IRRMIN00 PARM=UPDATE.

**Explanation:** During IPL RACF found that the database templates on the master primary database are not at the correct level.

**System action:** RACF ignores the templates on the database and uses the templates contained in the RACF Initialization load module instead.

**User response:** Run IRRMIN00 with PARM=UPDATE to apply the latest level of the templates to the
ICH580I  •  ICH584I

ICH580I  ICH584I

database. Until you do this you may see errors if you use IRRUT200 or BLKUPD to process the database, and the RACF Database unload utility may not unload all fields and segments.

Destination:  Descriptor code is 3. Routing codes are 2, 9, and 10.

ICH580I  WARNING: UACC(READ) WILL BE ASSUMED FOR PROGRAMS FROM SYS1.LINKLIB PROTECTED BY PROGRAM * OR **

Explanation:  The PROGRAM class profile * or ** has been specified with UACC(NONE) and data set SYS1.LINKLIB. The operating system must have access to programs in this data set. If any task obtains access using this profile through the UACC value, RACF will return to the caller an access value of READ. In addition, if ID(*) with ACC(NONE) is specified on the access list and is used for authorization, RACF will return to the caller an access value of READ.

System action:  Processing continues for SETROPTS. RACF will return to the caller an access value of READ for any program control access to SYS1.LINKLIB through UACC(NONE) or through ID(*) ACC(NONE).

User response:  Report this message to system administrator and system programmer. This use of UACC(NONE) or ID(*) ACC(NONE) with SYS1.LINKLIB might cause system problems.

Destination:  The descriptor code is 4. The routing code is 9.

ICH581I  DYNAMIC CLASS DESCRIPTOR TABLE PROCESSED

Explanation:  During RACF initialization, the dynamic class descriptor table was activated using class definitions from the CDT general resource class.

System action:  RACF initialization continues.

Destination:  Descriptor code is 4. Routing codes are 2 and 9.

ICH582I  RCVI STORAGE OBTAIN failure, return code = X'xxxxxxx'.

Explanation:  The attempt to obtain storage from subpool 245 for the RCVI (IRRPRCVI) failed. The STORAGE OBTAIN return code as specified by xxxxxxxx is given in hexadecimal.

System action:  RACF initialization continues. ICTX Java™ requests will fail with message ITY6521E. See z/OS Integrated Security Services EIM Guide and Reference for more information about ICTX Java requests and for a description of the ITY6521E message.

Operator response:  Report the exact text of this message to your system programmer.

ICH584I  ICH580I  ICH584I

System programmer response:  See z/OS MVS Programming: Assembler Services Reference IAR-XCT for the description of the return codes for the STORAGE OBTAIN macro. Determine the cause of the error, correct it, and try again. If the problem persists, contact the IBM support center.

Destination:  Descriptor code is 4. Routing codes are 2 and 9.

ICH583I  ICH584I

Explanation:  An unexpected return code was received from ICHEINTY while attempting to retrieve information from the specified profile-name in the LDAPBIND class. The ICHEINTY return code as specified by xxxxxxxx, and the reason code as specified by yyyyyyyy, are given in hexadecimal.

System action:  RACF initialization continues. The identity cache will use default configuration values:

- BASE segment: NOAPPLDATA
- PROXY segment: NOLDAPHOST, NOBINDDN
- EIM segment: NOLOCALREG
- ICTX segment: USEMAP, NODOMAP, NOMAPPINGREQUIRED, MAPPINGTIMEOUT(3600)

Operator response:  Report the exact text of this message to your system programmer.

System programmer response:  See z/OS Security Server RACF Macros and Interfaces for the description of the return and reason codes for the ICHEINTY macro. Determine the cause of the error, correct it, and try again. If the problem persists, contact your RACF Security Administrator.

Destination:  Descriptor code is 4. Routing codes are 2 and 9.

ICH584I  ICH580I  ICH584I

Explanation:  The ICHEINTY encountered a failing return code or reason code where:
- Type is the type of ICHEINTY (‘NEXT’ or ‘ALTER’)
- Profile is the profile name
  - for ICHEINTY ALTER the profile name is 9 to 16 characters in length.
  - for ICHEINTY NEXT a profile name might be 247 characters in length. A maximum of the first 20 characters of the profile name is presented in the message.

Operator response:  Report the exact text of this message to your system programmer.

System programmer response:  See z/OS MVS Programming: Assembler Services Reference IAR-XCT for the description of the return codes for the STORAGE OBTAIN macro. Determine the cause of the error, correct it, and try again. If the problem persists, contact the IBM support center.
Class is the General Resource class.
The dsname and volser indicate the database.

If there is an ICHEINTY NEXT failure, then because the IRRPLEX_ profiles are used to shield the database from corruption caused by incorrect database sharing, there might be a gap in that analysis.

If there is an ICHEINTY ALTER failure, then because the IRRPLEX_ profiles are used to shield the database from corruption caused by incorrect database sharing, there might be a gap in a future analysis.

System action: Initialization continues and in both cases processing continues.

Operator response: Contact your system programmer.

System programmer response: See z/OS Security Server RACF Macros and Interfaces for the description of the return and reason codes for the ICHEINTY macro.

When the system is available:

If there is an ICHEINTY ALTER failure, issue an RLIST command on the named profile. If this is successful issue an RVARY LIST command:

- If the RVARY LIST command indicates that the system is in data sharing mode, issue an RALTER command on the named profile and enter “DATA SHARING MODE” into the APPLDATA field.
- If the RVARY LIST command indicates that the system is in read-only mode and another system is using the database in data sharing mode, issue an RALTER command from that system on the named profile and enter “DATA SHARING MODE” into the APPLDATA field.
- If the RVARY LIST command does not indicate data sharing mode or read-only mode, issue an RALTER command on the named profile and enter “NON-DATA SHARING MODE” into the APPLDATA field.

If there is an ICHEINTY NEXT failure, issue a SEARCH command. For example:

SEARCH CLASS(GXFACILI) MASK(IRRPLEX_)

If there are still failures, issue an RDELETE command on the profile. If this is successful re-create the profile using the RDEFINE command, and either enter “DATA SHARING MODE” or “NON-DATA SHARING MODE” in the APPLDATA field, as determined by the RVARY command.

If there is an ICHEINTY NEXT failure, then because the IRRPLEX_ profiles are used to shield the database from corruption caused by incorrect database sharing, there might be a gap in that analysis. The database can become corrupted if:

- The RACF database is shared with systems that are outside the global resource serialization complex, and any of the sharing systems are in data sharing mode. Or,
- There are systems within the global resource serialization complex that are in data sharing mode, and any other sharing systems are in non-data sharing mode.

You can issue an RVARY list command to determine the database names and volser. This also indicates if the system is in data sharing mode. If the RACF database is incorrectly shared, run IRRUT200 against each data set and either move all sharing sysplexes out of data sharing mode into non-data sharing mode (RVARY NODATASHARE), or change your database sharing configuration. If the database is already corrupted, either restore an archived backup of the database, or contact your IBM support center.

If the message indicates that the ICHEINTY NEXT was run against the backup database, and you did not receive this message for the primary database, then if the backup database is intended to be the same as the primary database, resynchronize the primary and the backup databases using "IRRUT200 PARM=ACTIVATE".

Note: Ensure that the database you are using as the backup database is the correct database to be using with your primary database. The "IRRUT200 PARM=ACTIVATE" will overlay all the data within the specified backup data set. See z/OS Security Server RACF System Programmer’s Guide for more information about IRRUT200.

If the problem persists, contact your IBM support center.

Do not use RRSF to propagate the RDEFINE, RALTER, and RDELETE commands to other databases. If automatic command direction is enabled for the GXFACILI class, use the ONLYAT operand (on the RALTER, RDEFINE, and RDELETE commands) when you change IRRPLEX_sysplex-name profiles to prevent this propagation. ONLYAT must be used whether you are altering, Creating, or deleting the class GXFACILI IRRPLEX_sysplex-name profiles on a local or remote node.

Destination: Descriptor code is 4. Routing codes are 2 and 9.
Explanation: RACDEF encountered a failing return code or reason code. The creation of the named profile encountered a failure.

- **Profile** is the profile name
- **Class** is the General Resource class
- The **dsname** and **volser** indicate the database

Because the **IRRPLEX_** profiles are used to shield the database from corruption caused by incorrect database sharing, there might be a gap in a future analysis.

**System action:** Initialization continues.

**Operator response:** Contact your system programmer.

**System programmer response:** Issue an RVARY LIST command and update the APPLDATA field as appropriate:

- If the RVARY LIST command indicates that the system is in data sharing mode, issue an RDEFINE command on the named profile and enter “DATA SHARING MODE” into the APPLDATA field.
- If the RVARY LIST command indicates that the system is in read-only mode and another system is using the database in data sharing mode, issue an RDEFINE command from that system on the named profile and enter “DATA SHARING MODE” into the APPLDATA field.
- If the RVARY LIST command does not indicate data sharing mode or read-only mode, issue an RDEFINE command on the named profile and enter “NON-DATA SHARING MODE” into the APPLDATA field.

Do not use RRSF to propagate the RDEFINE, RALTER, and RDELETE commands to other databases. If automatic command direction is enabled for the GXFACILI class, use the ONLYAT operand (on the RALTER, RDEFINE, and RDELETE commands) when you change **IRRPLEX_sypplex-name** profiles to prevent this propagation. ONLYAT must be used whether you are altering, creating, or deleting the class **GXFACILI** **IRRPLEX_sypplex-name** profiles on a local or remote node.

If the problem persists, run **IRRUT200** (specifying INDEX FORMAT and MAP ALL in the SYSIN DD) against the data set within the database that contains the named profile, and contact your IBM support center.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.

---

**ICH586A**

**Explanation:** The APPLDATA field of one or more **IRRPLEX_sypplex-name** profiles indicates data sharing mode. Either the data set name table (ICHRDSNT) for this system specifies non-data sharing mode, or if the system is enabled for RACF sysplex communication, and this is not the first system to join the XCF group **IRRXCF00**, the current mode has been communicated by the group data set name table. The data sharing mode indicators within the **IRRPLEX_sypplex-name** profiles are incompatible with the non-data sharing mode requested for the initialization of this environment.

The **ICH600A** WTOR is issued after this message to obtain a response.

**Specify CONTINUE if:**

- the named profile is for this sysplex, and the named database is to be used in non-data sharing mode
- you have copied the database from an environment that shared the database with another sysplex in data sharing mode, but which is no longer true for this environment
- the sysplex was renamed, and is no longer in data sharing mode
- one or more **IRRPLEX_** profiles were manually altered or created incorrectly
  - the profile name indicates a sysplex that is not sharing the database
  - the APPLDATA field indicates data sharing mode (anything that begins with a “D”), but the system is not in data sharing mode
- an automated update of one or more **IRRPLEX_** profiles failed

**Specify FAILSOFT if:**

- the named profile is for this sysplex, the database is being used by this sysplex in data sharing mode, the system is not enabled for RACF sysplex communication, and you intended to IPL into data
sharing mode. Update the data set name table (ICHRDSNT) to request RACF sysexplex communication and data sharing mode, and then re-IPL the system.

- the profiles are correct, the database is being used by this sysexplex, or another sysexplex, in data sharing mode, and you must not use the database. Update the data set name table (ICHRDSNT) to request a different database, and then re-IPL the system.

**System action:** The system waits for the operator's reply.

**Operator response:** Respond to the ICH600A message or contact your system programmer.

**System programmer response:** If the identified database is being used in data sharing mode by another system, the database will become corrupted in the following situations:

- The other system is in another sysexplex.
- The other system is in this sysexplex, but this system is not enabled for RACF sysexplex communication (forcing the other system to use the databases and mode of the IRRXCF00 RACF sysexplex communication group).

You must specify FAILSOFT to protect the database.

**Notes:**

1. If the other system is in another sysexplex, either change the data set name table (ICHRDSNT) to use a different database, and then re-IPL the system, or issue an RVARY NODATASHARE command from the other sysexplex.

2. If the other system is in this sysexplex, but is not being used in data sharing mode, change the data set name table (ICHRDSNT) to request RACF sysexplex communication or data sharing mode, or both, and then re-IPL the system. This will cause the IRRXCF00 group to be joined and the RACF sysexplex communication group data set name table, which must be in the correct mode, to be used.

If the identified database is not being used in data sharing mode, specify CONTINUE. After initialization use the RDELETE or RALTER command on the IRRPLEX_sysplex-name profiles as appropriate. The IRRPLEX_sysplex-name profile for this sysexplex is updated automatically during initialization.

If the message indicates the backup database, and you did not receive this message for the primary database, then if the backup database is intended to be the same as the primary database, and you were able to specify ‘CONTINUE’ to this message, resynchronize the primary and the backup databases using "IRRUT200 PARM=ACTIVATE".

**Note:** Ensure that the database you are using as the backup database is the correct database to be using with your primary database. The "IRRUT200 PARM=ACTIVATE" will overlay all the data within the specified backup data set. See [z/OS Security Server RACF System Programmer's Guide](https://www.ibm.com) for more information about IRRUT200.

If the problem persists, contact your IBM support center.

Do not use RRSF to propagate the RDEFINE, RALTER, and RDELETE commands to other databases. If automatic command direction is enabled for the GXFACILI class, use the ONLYAT operand (on the RALTER, RDEFINE, and RDELETE commands) when you change IRRPLEX_sysplex-name profiles to prevent this propagation. ONLYAT must be used whether you are altering, creating, or deleting the class GXFACILI IRRPLEX_sysplex-name profiles on a local or remote node.

**Destination:** Descriptor code is 2. Routing code is 1.

### ICH587A

**THE RACF DATABASE WAS CHOSEN TO BE PROTECTED FROM CORRUPTION. NOW ENTERING FAILSOFT MODE.**

**Explanation:** You received either message ICH586A, ICH589A, ICH590A, or ICH591A. To protect your database from corruption you have chosen FAILSOFT.

**System action:** System continues initialization in FAILSOFT mode.

**Operator response:** Contact your system programmer.

**System programmer response:** Either specify a different database, or adjust the RACF sysexplex communication or data sharing mode request bits in the data set name table (ICHRDSNT), or both, and then re-IPL the system.

**Destination:** Descriptor code is 2. Routing code is 1.
CONTINUED USE OF DATABASE
DSNAME ON VOLUME VOLSER CAN RESULT IN DATABASE CORRUPTION
AND SYSTEM OUTAGE. IF ANY SYSTEM IS USING THE DATABASE
IN DATA SHARING MODE, AND ANY OTHER SYSTEM CONCURRENTLY
USES IT IN NON-DATA SHARING MODE, DATABASE CORRUPTION
WILL RESULT. YOU ARE INITIALIZING INTO DATA SHARING
MODE. PROFILE IRRPLEX_SYSPLEX-NAME, IN CLASS CLASS
INDICATES NON-DATA SHARING MODE. IF THE DATABASE IS NOT BEING USED BY
SYSTEMS OUTSIDE OF THIS SYSPLEX AND IS NOT BEING USED
BY SYSTEMS IN THIS SYSPLEX IN NON-DATA SHARING MODE, THEN
SPECIFY 'CONTINUE'. OTHERWISE SPECIFY 'NODATASHARE' AND THE
SYSTEM WILL INITIALIZE IN NON-DATA SHARING MODE.

Explanation: There are two explanations. Either:

1. If the named profile is for this sysplex and you are
changing your sysplex from non-data sharing mode
into data sharing mode, it is normal to receive this
message. To ensure that your database avoids
corruption you must determine if the databases are
being shared by other sysplex members that are not
enabled for RACF sysplex communication. Systems
that are enabled for RACF sysplex communication
are members of the XCF IRRXCF00 group.

First determine which systems are sysplex members,
but not IRRXCF00 group members. To display
sysplex members, enter the following command
from the master console:

D XCF,SYSPLEX

To display group members, enter the following
command from the master console:

D XCF,GROUP,IRRXCF00

Next issue an RVARY LIST command from the
systems in the sysplex that are not IRRXCF00 group
members. This indicates if the systems are using the
same databases as the systems within the group. If
there are systems using the same databases, this is
because either:

• The data set name table (ICHRRDSNT) of the other
systems sharing the databases did not specify
RACF sysplex communication during IPL (the
databases are used in the same mode as the
group). Or,

• This sysplex should not be in data sharing mode. Or,

• One of the systems has specified an incorrect
RACF database in the data set name table
(ICHRRDSNT)

Or:

2. The APPLDATA field of one or more
IRRPLEX_sysplex-name profiles, which are not for
this sysplex, indicates non-data sharing mode. This
system is currently changing to data sharing mode.
The data set name table (ICHRRDSNT) for this
system specifies data sharing mode. A system in
data sharing mode cannot safely share a database
with a system in another sysplex. Other IRRPLEX
profiles are incompatible with the data sharing
mode requested for the initialization of this
environment.

Note: If the message indicates a
IRRPLEX_sysplex-name profile, which is not
for this sysplex, you must also follow the
procedures in explanation 1 (assessing the
systems in this sysplex).

The ICH600A WTOR is issued after this message to
obtain a response.

Specify CONTINUE if:

• you have copied the database from an environment
that shared the database with another sysplex, but
which is no longer true for this environment.

• the sysplex was renamed, and the old
IRRPLEX_sysplex-name profile was detected.

• one or more IRRPLEX_ profiles were manually
altered or created. They indicate a sysplex (in the
profile name) that is not sharing the database.

• no other IRRPLEX_sysplex-name profiles were found,
and all sysplex members are enabled for RACF
sysplex communication.

To change the system into non-data sharing mode,
specify NODATASHARE if:

• the profiles are correct, and you must not use the
database in data sharing mode.

• there are sysplex members that are not enabled for
RACF sysplex communication but share this
database.

System action: The system waits for the operator’s
reply.

Operator response: Respond to the ICH600A message
or contact your system programmer.

System programmer response: If the identified
database is being used by another system, which is in
another sysplex, and this system requests data sharing
mode, the database will become corrupted. You must
specify NODATASHARE to protect the database. If you
must use data sharing mode on this system, but the
database is being used by another sysplex, then after
specifying NODATASHARE to the accompanying ICH600A WTOR, either:

- change the data set name table (ICHRDSNT) for the systems on the other sysplex, and then re-IPL those systems. Or,
- if, at this time, you cannot re-IPL the systems on the other sysplex, you can follow the directions for copying your database (primary and backup) in the z/OS Security Server RACF System Programmer’s Guide. This explains how to put the new copies onto different volumes. However, if you want to use databases with different names, the data set name table (ICHRDSNT) must still be changed to prevent this problem when you re-IPL the other systems.

The IRRPLEX_ profiles on the other sysplexes can be deleted from this database. You must then issue an RVARY DATASHARE command on this system.

If there are sysplex members that share this database, which are not enabled for RACF sysplex communication, you must also specify NODATASHARE to protect the database. If you need to use data sharing mode on this system, but the database is being used by a system, which is not enabled for RACF sysplex communication, then after specifying NODATASHARE to the accompanying ICH600A WTOR:

- if the other systems need to share this database, change the data set name table (ICHRDSNT) for systems that are not enabled for RACF sysplex communication, to request RACF sysplex communication, and then re-IPL the systems. Or,
- if the other systems do not need to share this database, they must use a different database. Follow the preceding instructions for changing databases when sharing from another sysplex.

You can then issue an RVARY DATASHARE command on this system.

If the identified database is not being used by a system that is either in another sysplex, or is on this sysplex but not enabled for RACF sysplex communication, specify CONTINUE. After initialization, you can use the RDELETE command to delete extraneous IRRPLEX_sysplex-name profiles. The IRRPLEX_sysplex-name profile for this sysplex is updated automatically during initialization.

If the message indicates the backup database, and you did not receive this message for the primary database, then if the backup database is intended to be the same as the primary database, and you were able to specify ‘CONTINUE’ to this message, resynchronize the primary and the backup databases using "IRRUT200 PARM=ACTIVATE".

Note: Ensure that the database you are using as the backup database is the correct database to be using with your primary database. The

"IRRUT200 PARM=ACTIVATE" will overlay all the data within the specified backup data set. See z/OS Security Server RACF System Programmer’s Guide for more information about IRRUT200.

If the problem persists, contact your IBM support center.

Do not use RRSF to propagate the RDEFINE, RALTER, and RDELETE commands to other databases. If automatic command direction is enabled for the GXFACILI class, use the ONLYAT operand (on the RALTER, RDEFINE, and RDELETE commands) when you change IRRPLEX_sysplex-name profiles to prevent this propagation. ONLYAT must be used whether you are altering, creating, or deleting the class GXFACILI IRRPLEX_sysplex-name profiles on a local or remote node.

Destination: Descriptor code is 2. Routing code is 1.

ICH589A CONTINUED USE OF DATABASE

DSNAME ON VOLUME VOLSER CAN RESULT IN DATABASE CORRUPTION AND SYSTEM OUTAGE. IF ANY SYSTEM IS USING THE DATABASE IN DATA SHARING MODE, AND ANY OTHER SYSTEM CONCURRENTLY USES IT IN NON-DATA SHARING MODE, DATABASE CORRUPTION WILL RESULT. YOU ARE Initializing INTO DATA SHARING MODE. PROFILE IRRPLEX_SYSPLEX-NAME, IN CLASS CLASS INDICATES NON-DATA SHARING MODE. IF THE DATABASE IS NOT BEING USED BY SYSTEMS OUTSIDE OF THIS SYSPLEX AND IS NOT BEING USED BY SYSTEMS IN THIS SYSPLEX IN NON-DATA SHARING MODE, THEN SPECIFY 'CONTINUE'. OTHERWISE SPECIFY 'FAILSOFT' AND THE SYSTEM WILL ENTER FAILSOFT MODE.

Explanation: There are two explanations. Either:

1. The named profile is for this sysplex. It is possible that an RVARY command or an IPL of a system that runs z/OS R10 or later, has changed the system mode to non-data sharing mode. However, an RVARY DATASHARE command has been issued from a system that runs a version before z/OS R10. Only z/OS R10 or later can automatically update the profile. As a result, the profile has not been updated and does indicate the actual system mode. Therefore, it is normal to receive this message. To ensure that your database avoids corruption you must determine if the databases are being shared by other sysplex members that are not enabled for RACF sysplex communication. Systems that are
enabled for RACF sysplex communication are members of the XCF IRRXCF00 group.

First determine which systems are sysplex members, but not IRRXCF00 group members. To display sysplex members, enter the following command from the master console:

```
D XCF,SYSPLEX
```

To display group members, enter the following command from the master console:

```
D XCF,GROUP,IRRXCF00
```

Next issue an RVARY LIST command from the systems in the sysplex that are not IRRXCF00 group members. This indicates if the systems are using the same databases as the systems within the group. If there are systems using the same databases, this is because either:

- The data set name table (ICHRDSNT) of the other systems sharing the databases did not specify RACF sysplex communication during IPL (the databases are used in the same mode as the group). Or,
- This sysplex should not be in data sharing mode. Or,
- One of the systems has specified an incorrect RACF database in the data set name table (ICHRDSNT).

Or:

2. The APPLDATA field of one or more IRRPLEX_sysplex-name profiles, which are not for this sysplex, indicates non-data sharing mode. This system is currently changing to data sharing mode.

The data set name table (ICHRDSNT) for this system specifies RACF sysplex communication, and because it is not the first system to join the XCF group IRRXCF00, the databases and the current mode have been communicated by the group data set name table, which has reported that the group is in data sharing mode. A system in data sharing mode cannot safely share a database with a system in another sysplex. Other IRRPLEX profiles are incompatible with the data sharing mode requested for the initialization of this environment.

**Note:** If the message indicates that a IRRPLEX_sysplex-name profile, which is not in this sysplex, you must also follow the procedures in explanation 1 (assessing the systems in this sysplex).

The ICH600A WTOR is issued after this message to obtain a response.

Specify CONTINUE if:

- you have copied the database from an environment that shared the database with another sysplex, but which is no longer true for this environment.
- the sysplex was renamed, and the old IRRPLEX_sysplex-name profile was detected.
- one or more IRRPLEX_profiles were manually altered or created incorrectly.
  - the profile name indicates a sysplex that is not sharing the database
- no other IRRPLEX_sysplex-name profiles were found, and all sysplex members are enabled for RACF sysplex communication.

Because other systems are enabled for RACF sysplex communication (members of the XCF IRRXCF00 group), and in data sharing mode, the database might be corrupted. When the system has completed IPL, it might be in FAILSOFT mode. If so, you must run IRRUT200 in copy and verify mode (specify SYSRACF and SYSUT1 DD) against the primary data sets of the database. If the database is corrupted, refresh it with a database that is not corrupted or contact your IBM service center. Either do not share the database outside of the systems on this sysplex, which are enabled for RACF sysplex communication, or do not allow data sharing mode.

Specify FAILSOFT if:

- the profiles are correct, and you must not use the database in data sharing mode.
- there are sysplex members that are not enabled for RACF sysplex communication but share this database.

**System action:** The system waits for the operator’s reply.

**Operator response:** Respond to the ICH600A message or contact your system programmer.

**System programmer response:** The database can become corrupted in the following situations:

- If the identified database is being used by another system, which is in another sysplex, and this system requests data sharing mode. Or,
- Because the IRRXCF00 group of this system is in data sharing mode.

To protect the database, specify FAILSOFT to enter FAILSOFT mode. You must run IRRUT200 in copy and verify mode (specify SYSRACF and SYSUT1 DD) against the data sets of the database. If the database is corrupted, refresh it with a database that is not corrupted or contact your IBM service center. Either do not share the database outside of the systems on this sysplex, which are enabled for RACF sysplex communication, or do not allow data sharing mode.

If the identified database is not being used by a system outside of this sysplex, specify CONTINUE. After
initialization use the RDELETE or RALTER command on the IRRPLEX_ profiles as appropriate. The IRRPLEX_ profile for this sysplex is updated automatically during initialization.

If the message indicates the backup database, and you did not receive this message for the primary database, then if the backup database is intended to be the same as the primary database, and you were able to specify ‘CONTINUE’ to this message, resynchronize the primary and the backup databases using ‘IRRUT200 PARM=ACTIVATE’.

Note: Ensure that the database you are using as the backup database is the correct database to be using with your primary database. The “IRRUT200 PARM=ACTIVATE” will overlay all the data within the specified backup data set. See ‘z/OS Security Server RACF System Programmer’s Guide’ for more information about IRRUT200.

If the problem persists, contact your IBM support center.

Do not use RRSF to propagate the RDEFINE, RALTER, and RDELETE commands to other databases. If automatic command direction is enabled for the GXFACILI class, use the ONLYAT operand (on the RALTER, RDEFINE, and RDELETE commands) when you change IRRPLEX_ profiles to prevent this propagation. ONLYAT must be used whether you are altering, creating, or deleting the class GXFACILI IRRPLEX_ profiles on a local or remote node.

Destination: Descriptor code is 2. Routing code is 1.

ICH590A

IF SYSTEMS FROM MULTIPLE SYSPLEXES USE THE DATABASE WITH MASTER DATASET DSNNAME ON VOLUME VOLUME IN DATA SHARING MODE, DATABASE CORRUPTION WILL RESULT. YOU ARE INITIALIZING INTO DATA SHARING MODE AND PROFILE IRRPLEX_SYSPLEX-NAME, IN CLASS CLASS INDICATES DATA SHARING MODE. IF THE DATABASE IS NOT BEING USED BY ANOTHER SYSPLEX, THEN SPECIFY ‘CONTINUE’. IF THE DATABASE IS INDEED BEING USED IN DATA SHARING MODE BY ANOTHER SYSPLEX SPECIFY ‘FAILSOFT’ AND THE SYSTEM WILL ENTER FAILSOFT MODE. IF THE DATABASE IS BEING USED BY ANOTHER SYSPLEX, BUT IN NON-DATA SHARING MODE SPECIFY ‘NODATASHARE’ AND THIS SYSTEM WILL INITIALIZE IN NON-DATA SHARING MODE.

Explanation: The APPLDATA field of one or more IRRPLEX_ profiles, which are not for this sysplex, indicates data sharing mode. This system is currently changing to data sharing mode. The data set name table (ICHRDSNT) for this system specifies data sharing mode. A database cannot be safely shared in data sharing mode with a system in another sysplex, neither can a system in data sharing mode share a database with a system that is not in data sharing mode.

The ICH600A WTO is issued after this message to obtain a response.

Specify CONTINUE if:
- you have copied the database from an environment that shared the database with another sysplex in data sharing mode, but which is no longer true for this environment
- the sysplex was renamed, and the old IRRPLEX_ profile was detected
- one or more IRRPLEX_ profiles were manually altered or created incorrectly
  - the profile name indicates a sysplex that is not sharing the database
  - the APPLDATA field indicates data sharing mode (anything that begins with a “D”), but the system is not in data sharing mode
- an automated update of one or more IRRPLEX_ profiles failed

Specify NODATASHARE if:
- another sysplex, which is in non-data sharing mode, is sharing this database

Specify FAILSOFT if:
- the profiles are correct, and you must not use the database in data sharing mode

System action: The system waits for the operator’s reply.

Operator response: Respond to the ICH600A message or contact your system programmer.

System programmer response: If the database is being used by another system, which is in data sharing mode in another sysplex, and this system requests data sharing mode, the database will become corrupted. If systems on other sysplexes use the database in data sharing mode, specify FAILSOFT to enter FAILSOFT mode. If systems on other sysplexes use the database in non-data sharing mode, specify NODATASHARE to enter non-data sharing mode.

If you specified FAILSOFT, then to correct the situation either change the data set name table (ICHRDSNT) to use a different database (if the database is being shared by another sysplex), or ensure that all systems sharing the database are in non-data sharing mode.

If the identified database is not being used by a system
outside of this sysplex, specify CONTINUE. After initialization use the RDELETE or RALTER command on the IRRPLEX_ profiles as appropriate. The IRRPLEX_ profile for this sysplex is updated automatically during initialization.

If the message indicates the backup database, and you did not receive this message for the primary database, then if the backup database is intended to be the same as the primary database, and you were able to specify ‘CONTINUE’ to this message, resynchronize the primary and the backup databases using 'IRRUT200 PARM=ACTIVATE'.

Note: Ensure that the database you are using as the backup database is the correct database to be using with your primary database. The "IRRUT200 PARM=ACTIVATE" will overlay all the data within the specified backup data set. See z/OS Security Server RACF System Programmer’s Guide for more information about IRRUT200.

If the problem persists, contact your IBM support center.

Do not use RRSF to propagate the RDEFINE, RALTER, and RDELETE commands to other databases. If automatic command direction is enabled for the GXFACILI class, use the ONLYAT operand (on the RALTER, RDEFINE, and RDELETE commands) when you change IRRPLEX_ profiles to prevent this propagation. You must use ONLYAT whether you are altering, creating, or deleting the class GXFACILI IRRPLEX_ profiles on a local or remote node.

Destination: Descriptor code is 2. Routing code is 1.

ICH591A IF SYSTEMS FROM MULTIPLE SYSPLEXES USE THE DATABASE WITH MASTER DATASET DSNNAME ON VOLUME VOLSER IN DATA SHARING MODE, DATABASE CORRUPTION WILL RESULT. YOU ARE INITIALIZING INTO DATA SHARING MODE AND PROFILE IRRPLEX_SYSPLEX-NAME, IN CLASS CLASS INDICATES DATA SHARING MODE. IF THE DATABASE IS NOT BEING USED BY ANOTHER SYSPLEX, THEN SPECIFY 'CONTINUE'. OTHERWISE SPECIFY 'FAILSOFT' AND THE SYSTEM WILL ENTER FAILSOFT MODE.

Explanation: The APPLDATA field of one or more IRRPLEX_ profiles, which are not for this sysplex, indicates data sharing mode. This system is currently changing to data sharing mode.

The data set name table (ICHRDSNT) for this system specifies RACF sysplex communication, and because it is not the first system to join the XCF group IRRXCF00, the databases and the current mode have been communicated by the group data set name table, which has reported that the group is in data sharing mode. A database cannot be safely shared in data sharing mode with a system in another sysplex, neither can a system in data sharing mode share a database with a system that is not in data sharing mode. Other IRRPLEX profiles are incompatible with the data sharing mode requested for the initialization of this environment.

The ICH600A WTOR is issued after this message to obtain a response.

Specify CONTINUE if:
- you have copied the database from an environment that shared the database with another sysplex in data sharing mode, but which is no longer true for this environment
- the sysplex was renamed, and the old IRRPLEX_ profile was detected
- one or more IRRPLEX_ profiles were manually altered or created incorrectly
  - the profile name indicates a sysplex that is not sharing the database
  - the APPLDATA field indicates data sharing mode (anything that begins with a “D”), but the system is not in data sharing mode
- an automated update of one or more IRRPLEX_ profiles failed

Because other systems are enabled for RACF sysplex communication (members of the XCF IRRXCF00 group), and data sharing mode, the database might be corrupted. When the system has completed IPL, it might be in FAILSOFT mode. If so, you must run IRRUT200 in copy and verify mode (specify SYSRACF and SYSUT1 DD) against the primary data sets of the database. If the database is corrupted, refresh it with a database that is not corrupted or contact your IBM service center. Either do not share the database outside of the systems on this sysplex, which are enabled for RACF sysplex communication, or do not allow data sharing mode.

Specify FAILSOFT if:
- the profiles are correct, and other sysplexes share the database

System action: The system waits for the operator’s reply.

Operator response: Respond to the ICH600A message or contact your system programmer.

System programmer response: If the database is being used by another system (in a different sysplex) that is in data sharing mode, the database might become corrupted. Because the IRRXCF00 group of this system is in data sharing mode, the database might be corrupted.
might exist one IRRPLEX profile. These profiles contain

Explanation:
For each unique sysplex name there
might exist one IRRPLEX profile. These profiles contain

Note: Ensure that the database you are using as the
backup database is the correct database to be using with your primary database. The
"IRRUT200 PARM=ACTIVATE" will overlay all the data within the specified backup data set.
See z/OS Security Server RACF System Programmer's Guide for more information about
IRRUT200.

If the problem persists, contact your IBM support center.

Do not use RRSF to propagate the RDEFINE, RALTER,
and RDELETE commands to other databases. If
automatic command direction is enabled for the
GXFACILI class, use the ONLYAT operand (on the
RALTER, RDEFINE, and RDELETE commands) when you change IRRPLEX Sysplex-name profiles to prevent
this propagation. ONLYAT must be used whether you are
altering, creating, or deleting the class GXFACILI
IRRPLEX.Sysplex-name profiles on a local or remote
node.

Destination: Descriptor code is 2. Routing code is 1.

ICH596I IN CLASS GXFACILI, AN IRRPLEX
PROFILE WAS ENCOUNTERED ON
THE DATABASE WITH MASTER
DATA SET DSNAME ON VOLUME
VOLSER, BUT THE SYSPLEX NAME
PORTION OF THE PROFILE NAME
WAS GREATER THAN 8
CHARACTERS. DATABASE SHARING
CHECKS HAVE IGNORED PROFILE
IRRPLEX_SYSPLEX-NAME.

Explanation: For each unique sysplex name there
might exist one IRRPLEX profile. These profiles contain

APPLDATA information, and are used by the routines,
which protect the database from being used in an
incorrect sharing environment, to prevent database
corruption. A sysplex name is limited to eight
characters in length. No information from this profile
was considered by the anti-corruption scheme.

A maximum of the first 20 characters of the profile
name is presented in the message.

System action: The system continues processing.

Operator response: Contact your system programmer.

System programmer response: IRRPLEX.Sysplex-name
profiles are used by the routines that protect the
database from bad sharing. If the names of profiles in
the GXFACILI class begin with “IRRPLEX_”, they
might remain if the environment has other uses for
them, and this message can be ignored.

If a sysplex, which runs at code levels less than in
z/OS R10, shares this database (RVARY LIST from the
security console), and you manually created the profile
to ensure that the code, which shields the database
from bad sharing, gets more pertinent information, you
must issue an RDELETE command on the profile and
reissue the command with a valid 8-character sysplex
name. Systems that run release z/OS R10 or later
automatically create and maintain these profiles.

If the message indicates the backup database, and you
did not receive this message for the primary database,
then if the backup database is intended to be the same
as the primary database, and you were able to specify
‘CONTINUE’ to this message, resynchronize the
primary and the backup databases using “IRRUT200
PARM=ACTIVATE”.

Note: Ensure that the database you are using as the
backup database is the correct database to be using with your primary database. The
"IRRUT200 PARM=ACTIVATE" will overlay all the data within the specified backup data set.
See z/OS Security Server RACF System Programmer's Guide for more information about
IRRUT200.

If the problem persists, contact your IBM support center.

Do not use RRSF to propagate the RDEFINE, RALTER,
and RDELETE commands to other databases. If
automatic command direction is enabled for the
GXFACILI class, use the ONLYAT operand (on the
RALTER, RDEFINE, and RDELETE commands) when you change IRRPLEX.Sysplex-name profiles to prevent
this propagation. ONLYAT must be used whether you are
altering, creating, or deleting the class GXFACILI
IRRPLEX.Sysplex-name profiles on a local or remote
node.

Destination: Descriptor code is 4. Routing codes are 2
and 9.
ICH597I IN CLASS GXFACILI, A PROFILE IRRPLEX_SYSPLEX-NAME WAS ENCOUNTERED ON THE DATABASE WITH MASTER DATA SET DSNAME ON VOLUME VOLSER. ITS APPLDATA IS NOT A RECOGNIZED VALUE.

Explanation: The APPLDATA field might indicate the RACF mode. If the profile is updated automatically, it contains "NON-DATA SHARING MODE" or "DATA SHARING MODE". If the APPLDATA field is set manually using RDEFINE or RALTER, the following values indicate the mode:

• If the first character is "N" it is an indication of non-data sharing mode.
• If the first character is "D" it is an indication of data sharing mode.

This APPLDATA field of the profile did not provide information for the support that protects the database from bad sharing.

System action: The system continues processing.

Operator response: Contact your system programmer.

System programmer response: It is assumed that the IRRPLEX_sysplex-name profile has been updated manually, and that the APPLDATA field has been updated incorrectly. An APPLDATA value that is not valid has no influence over the support to detect incorrect database sharing.

If you attempted to manually create a profile for a sysplex that shares the RACF database, but which is running at a level of RACF without the support required to detect incorrect database sharing, you entered incorrect APPLDATA. Systems that run release z/OS R10 or later, on a particular sysplex, automatically create and maintain these sysplex-related profiles.

If the profile is for the sysplex that received this message, and the system initialized in non-data sharing mode or data sharing mode, the APPLDATA is updated automatically. If the profile is not for this sysplex, you must issue an RALTER command and update the APPLDATA field of the named profile with a recognized value.

If the message indicates the backup database, and you did not receive this message for the primary database, then if the backup database is intended to be the same as the primary database, resynchronize the primary and the backup databases using "IRRUT200 PARM=ACTIVATE".

Note: Ensure that the database you are using as the backup database is the correct database to be using with your primary database. The "IRRUT200 PARM=ACTIVATE" will overlay all the data within the specified backup data set.


If the problem persists, contact your IBM support center.

Do not use RRSF to propagate the RDEFINE, RALTER, and RDELETE commands to other databases. If automatic command direction is enabled for the GXFACILI class, use the ONLYAT operand (on the RALTER, RDEFINE, and RDELETE commands) when you change IRRPLEX_sysplex-name profiles to prevent this propagation. ONLYAT must be used whether you are altering, creating, or deleting the class GXFACILI IRRPLEX_sysplex-name profiles on a local or remote node.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

ICH599I THE RESPONSE WAS UNRECOGNIZED. RESPECIFY RESPONSE.

Explanation: A WTOR has been issued, and an unrecognized response was proffered by the operator.

System action: The WTOR will be reissued.

Operator response: An unexpected response was made to the ICH600A WTOR to get a response to the scenario identified by one of the following WTOs: ICH586A, ICH588A, ICH589A, ICH590A, or ICH591A. Ensure that you use a complete keyword that the specific WTO is expecting.

Destination: Descriptor code is 4. Routing code is 2.

ICH600A VALID RESPONSES ARE ‘CONTINUE’ OR ‘NODATASHARE’ --or-- VALID RESPONSES ARE ‘CONTINUE’ OR ‘FAILSOFT’ --or-- VALID RESPONSES ARE ‘CONTINUE’, ‘FAILSOFT’ OR ‘NODATASHARE’

Explanation: One of the following WTOs: ICH586A, ICH588A, ICH589A, ICH590A, or ICH591A has been issued and this WTOR is requesting a response by the operator.

System action: If the response is one of the expected keywords, it is accepted. If the response is not one of the expected keywords, ICH599I is issued, and then ICH600A is reissued.

Operator response: Respond to the scenario proffered by one the following WTOs: ICH586A, ICH588A, ICH589A, ICH590A, or ICH591A. Ensure that you use a complete keyword that the specific WTO is expecting.

Destination: Descriptor code is 7. Routing code is 1.
RACF status messages

ICH702A ENTER PASSWORD TO {ACTIVATE | DEACTIVATE} RACF JOB=jobname, USER=userid.

Explanation: The user has issued the RVARY command to switch RACF status. The indicated job name and user ID are those of the person who issued the RVARY command. RACF routes this message to the security console and the master console.

System action: RACF waits for the operator to enter the password to allow the RVARY command to complete, or to enter another response (including a blank line) to cancel the command.

Operator response: Ensure that the request has been made by an authorized person within your installation. If it has, reply with the correct password; otherwise, enter a null response to cancel the RVARY command.

Destination: Descriptor code is 2. Routing codes are 1 and 9.

ICH703A ENTER PASSWORD TO SWITCH RACF {DATA SETS | MODE} JOB=jobname, USER=userid

Explanation: The RVARY command has been entered to switch RACF data sets or to change mode. The indicated job name and user ID are those of the issuer of the RVARY command. RACF routes this message to the security console and the master console.

System action: RACF waits for the operator to enter the password to allow the RVARY command to complete, or to enter another response (including a blank line) to cancel the command.

Operator response: Ensure that the request has been made by an authorized person within your installation. If it has, reply with the correct password; otherwise, enter a null response to cancel the command.

Destination: Descriptor code is 2. Routing codes are 1 and 9.
RACROUTE REQUEST=AUTH operator messages

ICH801I 'accessor' ATTEMPTING 'access-type'
ACCESS OF ENTITY 'name'

Explanation: A RACROUTE REQUEST=AUTH has been issued during a time when RACF processing is inactive. Because RACF is inactive, it allows access to the following resources:

- Resources accessed by started tasks that are marked as privileged or trusted in the RACF started procedures table (ICHRIN03)
- A user's own data sets
- Any other resources to which the operator allows access.

This message provides a record of the accesses to RACF-protected resources during the period when RACF is inactive.

The accessor represents a user ID, job name, or started-task name. The access-type represents the intended mode of system access (such as ALTER, CONTROL, UPDATE, or READ). The name is the name of the resource to which access was attempted, such as a data set name or a volume serial number. The name is one of the following names:

- The name as specified on the RACROUTE macro (if SETROPTS REALDSN is in effect)
- The name as modified according to RACF naming conventions (if SETROPTS NOREALDSN is in effect).

System action: If the accessor is a started task or a user accessing his own resource, RACF allows the access without operator intervention. If not, RACF issues message ICH802D requesting that the operator allow or deny the access.

Operator response: If RACF does not automatically allow the access, the following message ICH802D will ask the operator to allow or deny access.

Destination: Descriptor code is 2. Routing codes are 1, 2, 9, and 11.

ICH802D  REPLY Y OR N TO THE REQUEST.

Explanation: This message is displayed when RACF is inactive and a RACROUTE REQUEST=AUTH is issued on a protected resource. It follows message ICH801I that asks the operator to decide if the requester should be allowed access to the resource.

System action: The requesting task waits for the operator's reply. If the operator responds with N, the request is denied with, in some cases, an abend code. If the response is Y, the request is allowed, and processing continues.

Operator response: The preceding message ICH801I informs the operator about the resource being requested and the user ID, job name, or started-task name of the requester. The operator uses the installation regulations to decide whether to allow the access.

Destination: Descriptor code is 2. Routing codes are 1, 2, 9, and 11.
RACROUTE REQUEST=DEFINE operator messages

ICH901I  accessor ATTEMPTING access-type ACCESS OF ENTITY name IN CLASS class-name [NEW NAME new-name]

**Explanation:** RACF issued a RACROUTE REQUEST=DEFINE during a time when RACF processing was inactive. Because RACF is inactive, it allows access to the following resources:

- Resources accessed by started tasks that are marked as privileged or trusted in the RACF started procedures table (ICHRIN03)
- A user’s own data sets
- Any other resources to which the operator allows access.

This message informs the operator about a resource that RACF, in its inactive state, cannot update in the RACF database.

The variable accessor represents a user ID, job name, or started-task name. The variable access-type represents the intended mode of resource definition or update, such as DEFINE, ADDVOL, DELETE, or CHGVOL. The variable name is a RACF profile name, such as a data set name or a volume serial number. The variable class-name is one of the valid RACF class names. The variable new-name represents the new name of a data set being renamed.

**System action:** Processing continues with RACF inactive.

**Operator response:** Report this message to the system programmer and the RACF security administrator.

**Programmer response:** After RACF is reactivated, determine the status of the specified resource in the RACF database. If it is not valid, use the RACF commands to update the RACF database.

**Destination:** Descriptor code is 4. Routing codes are 1, 2, 9, and 11.

ICH903I  accessor SPECIFIED A 3-BYTE EXPiration DATE ON A RACROUTE REQUEST=DEFINE FOR A DATA SET NAME name.

**Explanation:** A RACROUTE REQUEST=DEFINE macro was invoked and specified the EXPDT keyword, which is the address of a 3-byte expiration date. A 3-byte expiration date can only specify a date in the range 1900-1999. This message is issued because the z/OS SYS1.PARMLIB member, ALLOCxx, contained the 2DGT_EXPDT statement specifying POLICY(FAIL).

**System action:** The RACROUTE REQUEST=DEFINE invocation fails with a SAF RC=8, RACF RC=8, RACF Reason Code = 80 (x'50').

**User response:** The program specifying the EXPDT keyword must be changed to use the EXPDTX keyword. If it is your program, change it. If it is not your program, have the supplier of the program change it.

**System programmer response:** Ensure that the program is changed before implementing POLICY(FAIL) on the 2DGT_EXPDT statement in the ALLOCxx SYS1.PARMLIB member.

**Destination:** Descriptor code is 4. Routing codes are 9 and 11.
Chapter 2. ICH messages for RACF commands

This section lists the command messages issued by RACF during the processing of the RACF commands. See “Recovery Procedures” in z/OS Security Server RACF System Programmer’s Guide for procedures to recover from errors that occur during the processing of the RACF commands.

The format of the command messages is:

ICHxxnnntt text

where:
ICH identifies the message as a RACF message.
xx is the command processor issuing the message.
nn is the message serial number.
t is the type code (I=information, A=action).
text is the text of the message.

The values for the xx field, which identifies the command processor, are:

xx Command
00 ADDGROUP
01 ADDUSER
02 CONNECT
03 REMOVE
04 DELUSER
05 DELGROUP
06 PERMIT
08 PASSWORD or PHRASE
09 ADDSD and DELSD
10 RDEFINE
11 RALTER
12 RDELETE
13 RLIST
14 SETROPTS
15 RVARY
20 ALTGROUP
21 ALTUSER
22 ALTDSD
30 LISTUSER
31 SEARCH
32  LISTGRP
35  LISTDSD
ADDGROUP command messages

ICH00002I  NOT AUTHORIZED TO ISSUE ADDGROUP

Explanation:  One of the following conditions is true:
• RACF is inactive.
• You are not defined to RACF and cannot issue RACF commands.
• You are not defined to RACF with sufficient authority to issue this command.

System action:  Command processing stops.

User response:  If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response:  If the user is not defined to RACE, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information on adding or altering user profiles or the authority required to issue the indicated command, see z/OS Security Server RACF Command Language Reference.

ICH00003I  UNABLE TO ACCESS group-name

Explanation:  RACF cannot find the description of the indicated superior group.

System action:  Command processing stops.

ICH00004I  COMMAND ENDED DUE TO ERROR

Explanation:  An ESTAE recovery environment cannot be established.

System action:  Command processing stops.

User response:  Report this message to your system programmer. Include the following information:
• The message ID
• The exact wording of the command you entered
• The date and time you entered the command.

System programmer response:  Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

ICH00005I  RECOVERY UNSUCCESSFUL

Explanation:  As issued, the ADDGROUP command began to update more than one profile in the RACF database. However, a system or RACF failure occurred during command processing.

System action:  To prevent discrepancies among profiles, RACF attempted to back out any changes already made to profiles. However, not all changes can be backed out. This message follows message ICH00006I.

User response:  Report this message and the exact text of message ICH00006I to your system programmer.

Problem Determination:  The RACF utility programs may be needed to correct the RACF database.

ICH00006I  group-name NOT ADDED -or- group-name AND REMAINING GROUPS NOT ADDED -or- GROUP(S) NOT ADDED

Explanation:  The group indicated in the message was not added. The remaining groups will be added.

ICH00007I  INSUFFICIENT AUTHORITY TO SUPERIOR GROUP

Explanation:  You do not have sufficient authority to issue the ADDGROUP command.

System action:  Command processing stops.

User response:  See your RACF security administrator.

ICH00008I  OWNER-GROUP AND SUPERIOR GROUP MUST BE THE SAME

Explanation:  When the owner of a group is another group, the owning group and the superior group must be the same.

System action:  Command processing stops.

ICH00009I  NOT AUTHORIZED TO INCLUDE DFP SEGMENT IN GROUP PROFILE group-name  GROUP PROFILE WAS NOT DEFINED

Explanation:  You are not authorized to add DFP segment information to the specified group profile.

System action:  Command processing stops with no update to the specified group profile.

User response:  See your RACF security administrator for authority to the DFP segment of this group profile.

RACF Security Administrator Response:  You can use field-level access checking to allow this user to add DFP segment information. For a description of field-level access checking, see z/OS Security Server RACF Security Administrator’s Guide.

ICH00010I  Group group-name is specified multiple times on the command.

Explanation:  You are not allowed to specify the same group more than once on the command.
ICH00011I

**System action:** The duplicate group is identified. No
group is added.

**User response:** Reissue the command without the
duplicate group name.

---

ICH00011I      No group is added.

**Explanation:** See accompanying message ICH00010I.

**System action:** Command processing ends with no
group added.

**User response:** Using the information in message
ICH00010I, correct the syntax and reissue the
command.
### ADDUSER command messages

**ICH01001I NOT AUTHORIZED TO SPECIFY [AUDITOR, OPERATIONS, SPECIAL], OPERAND IGNORED**

**Explanation:** You do not have sufficient authority to specify the keywords shown.

**System action:** The command continues with the attributes NOOPERATIONS, NOSPECIAL, or NOAUDITOR.

**User response:** Report this message to your RACF security administrator.

**ICH01002I NOPASSWORD OPERAND IGNORED**

**Explanation:** You specified the NOPASSWORD operand with the PHRASE operand. A user must have a password when a password phrase is specified.

**System action:** RACF ignores the NOPASSWORD operand.

**ICH01003I NOT AUTHORIZED TO SPECIFY CLAUTH FOR [TAPEVOL, USER, DASDVOL, TERMINAL], CLASS IGNORED**

**Explanation:** You do not have sufficient authority to specify CLAUTH for the indicated class.

**System action:** RACF ignores this class and continues with the next class or operand.

**User response:** Report this message to your RACF security administrator.

**ICH01004A ENTER OPERATOR IDENTIFICATION CARD**

**Explanation:** You have specified the OIDCARD operand. This message is requesting that you enter the operator identification card for the user being defined so that the information on it can be put into the user profile.

**System action:** Command processing waits for you to enter the operator identification card.

**ICH01005I NOT AUTHORIZED TO ISSUE ADDUSER**

**Explanation:** One of the following conditions is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

**System action:** Command processing stops.

**User response:** If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

**RACF Security Administrator Response:** If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or the authority required to issue the indicated command, see z/OS Security Server RACF Command Language Reference.

**ICH01006I COMMAND ENDED DUE TO ERROR TERMINAL TYPE NOT SUPPORTED**

**Explanation:** You specified the OIDCARD operand, but when the operator identification card was entered, it cannot be verified because it was entered on a terminal that is not supported.

**System action:** Command processing stops.

**ICH01007I COMMAND ENDED DUE TO ERROR UNABLE TO PROMPT FOR OIDCARD**

**Explanation:** You specified the OIDCARD operand, but TSO/E was unable to prompt you to enter the operator identification card.

**User response:** Be sure you are executing the command in the foreground and in prompt mode.

**ICH01008I COMMAND ENDED DUE TO ERROR UNABLE TO ESTABLISH ESTAE**

**Explanation:** An ESTAE recovery environment cannot be established.

**System action:** Command processing stops.

**User response:** Report this message to your system programmer. Include the following information:

- The message ID
- The exact wording of the command you entered
- The date and time you entered the command.

**System programmer response:** Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

**ICH01009I RECOVERY UNSUCCESSFUL**

**Explanation:** As issued, the ADDUSER command began to update more than one profile in the RACF database. However, a system or RACF failure occurred during command processing.

**System action:** To prevent discrepancies among profiles, RACF attempted to back out any changes already made to profiles. However, not all changes can
be backed out. This message follows message ICH01010I.

User response: Report this message and the exact text of message ICH01010I to your system programmer.

Problem Determination: The RACF utility programs may be needed to correct the RACF database.

ICH01010I userid NOT ADDED -or- userid AND REMAINING USERS NOT ADDED -or- USER(S) NOT ADDED

Explanation: The indicated user ID was not added. The remaining user IDs will be added. This message is also issued if the SETROPTS NJEUSERID or SETROPTS UNDEFINEDUSER is used on an ADDUSER.

ICH0111I INSUFFICIENT AUTHORITY

Explanation: You do not have sufficient authority to issue the ADDUSER command.

System action: Command processing stops.

User response: See your RACF security administrator.

ICH01012I COMMAND ENDED DUE TO ERROR PUTGET ERROR RETURN CODE IS return-code

Explanation: You specified the OIDCARD operand, but the TSO/E PUTGET service routine failed with the indicated return code while trying to read the operator identification card. For an explanation of the return code, see z/OS TSO/E Programming Services.

ICH01013I COMMAND PROCESSING TERMINATED, NO {SECLEVELS | CATEGORIES} FOUND

Explanation: RACF cannot validate the name you specified on the SECLEVEL or ADDCATEGORY parameter. This happened for one of two reasons:
• There is no SECLEVEL or CATEGORY profile.
• A profile is defined but it does not contain any members.

System action: Command processing stops.

ICH01015I COMMAND PROCESSING COMPLETED BUT UNABLE TO UPDATE ‘SYS1.BROADCAST’.

Explanation: RACF cannot update the TSO/E data set SYS1.BROADCAST.

System action: The ALTUSER command completed successfully and the user profile in the RACF database has been updated.

User response: Report this message to your system programmer.

System programmer response: Check to ensure that data set SYS1.BROADCAST exists on the system and is available to RACF.

ICH01016I SIZE SPECIFIED GREATER THAN MAXSIZE, SIZE ADJUSTED TO EQUAL TO MAXSIZE

Explanation: The specified SIZE is greater than the maximum allowable size, as specified on the MAXSIZE operand.

System action: RACF adds a user profile, but adjusts SIZE to equal the MAXSIZE operand.

User response: To change the SIZE or MAXSIZE operands for this user profile, use the ALTUSER command.

ICH01017I ADDUSER failed. SECLABEL seclabel-name is not currently defined to RACF.

Explanation: There is no profile in class SECLABEL whose name matches the security label indicated in the message.

System action: Command processing stops.

User response: Check the spelling of the value specified on the security label operand. If it is correct, define a profile with that name in the SECLABEL class. If you cannot define the profile, report the exact text of this message to your RACF security administrator.

ICH01019I User usrename is assigned an OMVS UID, but default group grpname does not have a GID. Processing continues.

Explanation: This is a warning message that gets issued if a user with an OMVS UID gets added and has a default group that does not have a GID.

User response: This usage violates documented rules. Either the default group should be assigned a GID, or the UID should be removed from the user profile.

RACF Security Administrator Response: Follow documented guidelines to assure that default groups for (OMVS users with UIDs) have GIDs assigned.

ICH01020I PASS PHRASE CHANGE REJECTED BY INSTALLATION PASS PHRASE EXIT

Explanation: The proposed password phrase, as specified in the PHRASE operand on the ADDUSER command, has been rejected by the installation password phrase exit, ICHPWX11.

System action: RACF ignores the operand and continues command processing with the next operand.

User response: See your RACF security administrator.
for the rules regarding new password phrases.

ICH01021I NEW PASS PHRASE REJECTED BY RACF RULES

Explanation: You specified a potential password phrase that does not adhere to the following syntax rules:

• The user ID is not part of the password phrase.
• At least 2 alphabets are specified (A - Z, a - z).
• At least 2 non-alphabets are specified (numerals, punctuation, special characters).
• No more than 2 consecutive characters are identical.

System action: RACF ignores the operand and continues command processing with the next operand.

User response: Try again with a different password phrase.
CONNECT command messages

**ICH02001I**  COMMAND ENDED DUE TO ERROR

**Explanation:** An ESTAE recovery environment cannot be established.

**System action:** Command processing stops.

**User response:** Report this message to your system programmer. Include the following information:
- The message ID
- The exact wording of the command you entered
- The date and time you entered the command.

**System programmer response:** Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

**ICH02002I**  RECOVERY UNSUCCESSFUL

**Explanation:** A system or RACF failure occurred when the CONNECT command began to update more than one profile in the RACF database.

**System action:** To prevent discrepancies among profiles, RACF attempted to back out any changes already made to profiles. However, not all changes can be backed out. This message follows message ICH02003I.

**User response:** Report this message and the exact text of message ICH02003I to your system programmer.

**Problem Determination:** The RACF utility programs may be needed to correct the RACF database.

**ICH02003I**  **userid** NOT CONNECTED -or- userid AND REMAINING USERS NOT CONNECTED

**Explanation:** The indicated user ID and all remaining user IDs were not connected because of an error in RACF processing.

**ICH02004I**  INSUFFICIENT AUTHORITY TO GROUP

**Explanation:** You do not have sufficient authority to issue the CONNECT command.

**System action:** Command processing stops.

**User response:** See your RACF security administrator.

**ICH02005I**  **userid** CONNECTION NOT MODIFIED

**Explanation:** The indicated user ID was found in the group’s access list, but either no connect profile was found or an error occurred while attempting to modify the connect profile.

**System action:** Command processing continues with the next user ID in the list.

**ICH02006I**  NOT AUTHORIZED TO ISSUE CONNECT

**Explanation:** One of the following conditions is true:
- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

**System action:** Command processing stops.

**User response:** If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

**RACF Security Administrator Response:** If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or the authority required to issue the indicated command, see z/OS Security Server RACF Command Language Reference.

**ICH02007I**  **userid** NOT AUTHORIZED TO SPECIFY {SPECIAL | OPERATIONS | AUDITOR}, OPERAND IGNORED

**Explanation:** You do not have sufficient authority to specify the operand indicated.

**System action:** RACF ignores the operand. Command processing continues with the next operand.

**User response:** Report this message to your RACF security administrator.

**ICH02008I**  AUTHORITY SPECIFIED GREATER THAN THE COMMAND USER

**Explanation:** You have specified a group authority on the AUTHORITY operand of the CONNECT command that is greater than your own.

**System action:** Command processing stops.

**User response:** Check the spelling of the group authority you specified.

**ICH02009I**  NOT AUTHORIZED TO ALTER **userid** TO [NOSPECIAL | NOOPERATIONS | NOAUDITOR]

**Explanation:** You do not have sufficient authority to modify the existing group connection for the indicated user ID. You cannot specify the indicated operand.
System action: RACF ignores the operand. Command processing continues with the next operand.

User response: Report this message to your RACF security administrator.

RACF Security Administrator Response: See z/OS Security Server RACF Command Language Reference for the authority required to issue the CONNECT command with the indicated operand.

ICH02010I  AUTHORITY NOT ALTERED FOR userid

Explanation: You specified the AUTHORITY operand but an error occurred while attempting to modify the group authority field in the group profile for the indicated user ID.

System action: Command processing continues with the next operand.

ICH02011I  OWNER SPECIFIED IS NOT A RACF DEFINED USER OR GROUP

Explanation: The user ID or group name specified on the OWNER operand is not defined to RACF.

System action: Command processing stops.

ICH02012I  'RESUME' IGNORED. userid NOT CURRENTLY REVOKED

Explanation: The indicated user ID is not currently revoked.

System action: RACF ignores the specification of a future date with the RESUME operand. Command processing continues with the next operand.

ICH02013I  'REVOKE' IGNORED. userid IS CURRENTLY REVOKED

Explanation: REVOKE was specified with a date, but the user is already revoked.

System action: Command processing continues with the next operand.
**REMOVE command messages**

**ICH03002I**  
**userid WAS NOT CONNECTED TO GROUP**

**Explanation:** The indicated user ID was not connected to the group, therefore, no processing can be done for the user.

**System action:** Command processing continues with the next user ID in the list.

**ICH03003I**  
**INSUFFICIENT AUTHORITY TO GROUP, NO USERS REMOVED**

**Explanation:** You do not have sufficient authority to issue the REMOVE command.

**System action:** Command processing stops.

**User response:** See your RACF security administrator.

**ICH03004I**  
**COMMAND ENDED DUE TO ERROR**

**Explanation:** An ESTAE recovery environment cannot be established.

**System action:** Command processing stops.

**User response:** Report this message to your system programmer. Include the following information:
- The message ID
- The exact wording of the command you entered
- The date and time you entered the command.

**System programmer response:** Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

**ICH03005I**  
**userid CANNOT BE NEW OWNER AS USER WAS SPECIFIED TO BE REMOVED**

**Explanation:** An attempt was made to remove the indicated user ID from a group. However, the user was also specified as the new owner of the group data set profiles and must stay connected to the group.

**System action:** Those user IDs that own group data set profiles are not removed. All remaining user IDs that do not own group data set profiles are removed.

**ICH03006I**  
**userid NOT REMOVED -or- userid AND REMAINING USERS NOT REMOVED -or- USER(S) NOT REMOVED**

**Explanation:** The indicated user ID was not removed.

**System action:** If this message follows ICH03004I, then no further users are removed.

**ICH03007I**  
**SOME GROUP DATA SET OWNERS WERE CHANGED**

**Explanation:** The command was not completed successfully. An error was detected while removing the user indicated in message ICH03006I.

**System action:** Some of the group data sets owned by the user were modified to reflect the new owner. This was not completed.

**User response:** Use the LISTDSD command to determine the status of the group data sets.

**ICH03008I**  
**NOT AUTHORIZED TO ISSUE REMOVE**

**Explanation:** One of the following conditions is true:
- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

**System action:** Command processing stops.

**User response:** If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

**RACF Security Administrator Response:** If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or the authority required to issue the indicated command, see z/OS Security Server RACF Command Language Reference.

**ICH03014I**  
**group-name IS DEFAULT GROUP, userid NOT REMOVED**

**Explanation:** A user cannot be removed from the default group. Specify the group name again or use the DELUSER command to remove the user from the default group.

**ICH03021I**  
**OWNER REQUIRED FOR GROUP DATASETS, userid NOT REMOVED**

**Explanation:** The indicated user ID is the owner of group data sets and cannot be removed because another owner was not specified or was invalid.

**System action:** The command continues with the next user ID.

**ICH03025I**  
**OWNER SPECIFIED NOT CONNECTED TO GROUP**
Explanation: The owner specified on the command is not connected to the group.

System action: If any user ID specified to be removed owns group data sets, message ICH03021I will be issued. The command continues with the next user ID.

ICH03026I  INSTALLATION EXIT FAILED
            REMOVE REQUEST FOR userid

Explanation: The command preprocessing exit routine ICHCCX00 issued a return code of 8, indicating that RACF should fail the REMOVE request for the indicated user ID.

System action: Processing of the REMOVE command continues with the next user ID specified.

User response: Report this message to your system programmer.
DELUSER command messages

ICH04001I  ERROR LOCATING userid
Explanation: The indicated user ID is not defined in the RACF database.
System action: Command processing continues with the next user specified.

ICH04002I  ERROR DELETING userid
Explanation: An error occurred while deleting the indicated user ID. The user profile may be in an inconsistent state.
System action: Command processing continues with the next user specified.

ICH04004I  COMMAND ENDED DUE TO ERROR
Explanation: An ESTAE recovery environment cannot be established.
System action: Command processing stops.
User response: Report this message to your system programmer. Include the following information:
• The message ID
• The exact wording of the command you entered
• The date and time you entered the command.
System programmer response: Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

ICH04006I  userid NOT DELETED -or- userid AND REMAINING USERS NOT DELETED -or- USER(S) NOT DELETED
Explanation: The indicated user ID was not deleted because of an error in command processing. The remaining user IDs also may not have been deleted, depending on the type of error.

ICH04007I  INSTALLATION EXIT FAILED DELETE REQUEST FOR userid
Explanation: The command preprocessing exit routine ICHCCX00 issued a return code of 8, indicating that RACF should fail the DELUSER request for the indicated user ID.
System action: Processing of the DELUSER command continues with the next user ID specified.
User response: Report this message to your system programmer.

ICH04009I  userid CANNOT BE DELETED. DATA SET PROFILES STILL EXIST.
Explanation: The indicated user ID was not deleted from the RACF database because the data set profiles still exist for the user. All data set profiles for this user must be deleted before the user ID can be deleted.
System action: Command processing continues with the next user.

ICH04010I  NOT AUTHORIZED TO ISSUE DELUSER
Explanation: One of the following conditions is true:
• RACF is inactive.
• You are not defined to RACF and cannot issue RACF commands.
• You are not defined to RACF with sufficient authority to issue this command.
System action: Command processing stops.
User response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or the authority required to issue the indicated command, see z/OS Security Server RACF Command Language Reference.

ICH04011I  Deletion of IBMUSER not allowed.
Explanation: User IBMUSER may not be deleted from the RACF database.
System action: RACF attempts to delete the rest of the users (if any) specified on the command line.

ICH04012I  User ID userid cannot be deleted. One or more user ID associations exist.
Explanation: A user ID cannot be deleted while user ID associations between the user ID being deleted and other user IDs are in effect. You must delete the user ID associations before deleting the user ID.
System action: The DELUSER command is unsuccessful; processing ends.
User response: Delete all user ID associations between the user ID being deleted and other user IDs by using the RACLINK command with the UNDEFINE operand. If you want to view the user ID associations between the user ID being deleted and other user IDs, issue a RACLINK command with the LIST operand.
ICH04013I  User ID userid cannot be deleted. User ID association retrieval failed.

Explanation: The indicated user ID cannot be deleted because an error occurred while RACF attempted to retrieve user ID association information for the user ID. The status of user ID associations between the user ID being deleted and other user IDs is unknown. A user ID with user ID associations defined with other user IDs cannot be deleted. This message is accompanied by messages IRRT004I, IRRT005I, or IRRT006I, which explain the error in more detail.

System action: The DELUSER command is unsuccessful; processing ends.

User response: Verify that the DELUSER command specified the correct user IDs to be deleted. If it did not, retry the command. If the correct user IDs were supplied, refer to the accompanying messages for more information.

ICH04014I  Unable to delete certificate certificate-name.

Explanation: An error occurred when DELUSER attempted to delete digital certificate profile certificate-name in the DIGTCERT class for the user specified on the DELUSER command.

System action: DELUSER command processing ends.

User response: Check for additional error messages related to the problem. Issue the RACDCERT command with the LIST keyword to examine the user's certificate information. Try to issue the RACDCERT command with the DELETE keyword to delete the certificate information for this user.

ICH04015I  Unable to delete ring ring-name.

Explanation: An error occurred when DELUSER attempted to delete ring profile ring-name in the DIGTRING class for the user specified on the DELUSER command.

System action: DELUSER command processing ends.

User response: Check for additional error messages related to the problem. Issue the RACDCERT command with the LISTSTRING keyword to examine the user's digital certificate key ring information. Try to issue the RACDCERT command with the DELRING keyword to delete the ring information for this user.

ICH04016I  Unable to remove associated certificate mapping mapping-profile-name.

Explanation: An error occurred when DELUSER attempted to delete a DIGTNMAP mapping profile, mapping-profile-name, or remove the filter associated with the user being deleted from this mapping profile. Profile names in the DIGTNMAP class are hashed. The actual names used to create the hash are part of the data within the profile. The message contains the hashed profile name. If the mapping-profile-name does not appear in the message, an error was encountered attempting to retrieve the names of the mapping profiles from the user profile.

System action: DELUSER command processing ends.

User response: Check for additional error messages related to the problem. Issue the RACDCERT command with the LISTMAP keyword to examine the user's mapping information. Attempt to issue the RACDCERT command with the DELMAP keyword to delete the information for this user.

ICH04017I  Warning: error locating certificate information for this user. Templates might be downlevel.

Explanation: An error occurred when DELUSER attempted to check for digital certificate information associated with the user being deleted. The return codes received by DELUSER indicate that the most likely cause of the problem is downlevel templates. That is, the copy of the templates currently in storage is at a lower level than the level on which you are running.

System action: DELUSER command processing continues.

User response: If the RACDCERT command was not used to define certificates or associate certificate mappings with this user, DELUSER continues processing and should complete successfully. Ask your system programmer to run IRRMIN00 with PARM=UPDATE to pick up the correct templates, and to schedule an IPL of this system to update the in-storage templates.

If there is certificate information associated with this user, it was added from a system with the correct template level. Issue the RACF SET LIST command on all systems sharing the RACF database to determine the level of their in-storage templates. Issue additional DELUSER commands from the system with the correct template level, and run the remove ID utility from that system to identify residual DIGTCERT, DIGTCRIT and DIGTNMAP profiles associated with the user deleted. Ask your system programmer to schedule an IPL of the system where the DELUSER failed to pick up the correct templates.

ICH04018I  userid cannot be deleted. Distributed identity mapping profiles are associated with this user.

Explanation: The indicated user ID has not been deleted from the RACF database because the user profile indicates that distributed identity mapping profiles still exist for the user in the IDIDMAP class. All associated mapping profiles for this user must be
deleted using the RACMAP command before the user ID can be deleted.

**System action:**  DELUSER command processing ends for this user.

**User response:**  Issue the RACMAP command with the LISTMAP keyword to examine the user's mapping information. Issue the RACMAP command with the DELMAP keyword to delete the distributed identity information in the user profile and the associated mapping profiles for this user.
DELGROUP command messages

ICH05001I  ERROR LOCATING group-name
Explanation: The specified group name is not defined in the RACF database.
System action: Command processing continues with the next group.

ICH05002I  COMMAND ENDED DUE TO ERROR
Explanation: An ESTAE recovery environment cannot be established.
System action: Command processing stops.
User response: Report this message to your system programmer. Include the following information:
- The message ID,
- The exact wording of the command you entered,
- The date and time you entered the command.
System programmer response: Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

ICH05004I  group-name NOT DELETED -or-
            group-name AND REMAINING
            GROUPS NOT DELETED -or-
            GROUP(S) NOT DELETED
Explanation: The group indicated in the message and all remaining groups were not deleted.

ICH05005I  NOT AUTHORIZED TO ISSUE
            DELGROUP
Explanation: One of the following conditions is true:
- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.
System action: Command processing stops.
User response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or the authority required to issue the indicated command, see z/OS Security Server RACF Command Language Reference.

ICH05006I  group-name CANNOT BE DELETED,
            GROUP DATA SETS STILL DEFINED
            TO RACF
Explanation: The group indicated in the message was not deleted from the RACF database because there are still group data sets associated with the group. A group cannot be deleted until RACF-protection is removed from the group data sets with the DELDSD command.
System action: Command processing continues with the next group.

ICH05007I  INSTALLATION EXIT FAILED DELETE
            REQUEST FOR group-name
Explanation: The command preprocessing exit routine ICHCCX00 issued a return code of 8, indicating that RACF should fail the DELGROUP request for the indicated group name.
System action: Processing of the DELGROUP command continues with the next group name specified.
User response: Report this message to your system programmer.

ICH05008I  WARNING group-name is a universal
            group. Run the remove ID utility to
            remove all users from the group.
Explanation: The group you are deleting is a universal group that does not list all members of the group within the group profile. If you do not use the REMOVE command to remove the users from the group, some user profiles can still contain a group connection for the group being deleted.
System action: Processing of the DELGROUP command continues.

RACF Security Administrator Response: If you are executing the DELGROUP and any REMOVE commands created by the remove ID utility, then no action is required.
Otherwise, to ensure you have removed all users from the group, run the remove ID utility (IRRRID00), specifying the group name, and execute the resulting commands.
PERMIT command messages

ICH06001 ICH06008

ICH06001I name ALREADY AUTHORIZED TO RESOURCE - ACCESS UNCHANGED

Explanation: The indicated name (user ID or group name) in the FROM resource's access list is already on the access list of the TO resource.

System action: Command processing continues with the next name in the FROM resource's access list.

ICH06002I name NOT AUTHORIZED, DELETE IGNORED

Explanation: The indicated name (user ID or group name) is not on the access list of the specified resource, and the request to delete the name from the access list is ignored.

System action: Command processing continues with the next operand.

User response: Check the spelling of the name indicated in the message. If the name is spelled correctly, check the spelling of the profile whose access list you want to change. For general resource profiles, check the class name and also the profile name.

ICH06003I NOT AUTHORIZED TO ISSUE command-name

Explanation: One of the following conditions is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System action: Command processing stops.

User response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or the authority required to issue the indicated command, see z/OS Security Server RACF Command Language Reference.

ICH06004I profile-name NOT DEFINED TO RACF

Explanation: The specified profile name is not defined to RACF.

Note: If you enter the PERMIT command for a fully qualified generic profile (one whose name has no generic characters), but you do not specify the GENERIC operand, RACF issues this message. This occurs because, without the GENERIC operand, RACF looks for a discrete profile of that name. For example, if there is a fully qualified generic profile named ABC.DATA, and you enter the following command:

PERMIT 'ABC.DATA' ACCESS(READ) ID(JOE)

RACF looks for a discrete profile named ABC.DATA and, if there is none, issues this message (ICH06004I ABC.DATA NOT DEFINED TO RACF). To identify for RACF the generic profile, specify the GENERIC operand as follows:

PERMIT 'ABC.DATA' ACCESS(READ) ID(JOE) GENERIC

Likewise, when using the FROM operand to copy an access list from a fully qualified generic profile, specify the FGENERIC operand to identify the fully qualified generic profile to RACF.

System action: Command processing stops.

ICH06005I COMMAND ENDED DUE TO ERROR

Explanation: A RACF manager error occurred. This message is accompanied by a message explaining the error.

System action: Command processing stops.

ICH06006I NOT AUTHORIZED TO profile-name

Explanation: You are not authorized to alter or copy the access list of the resource indicated by profile-name.

System action: Command processing stops.

ICH06007I name NOT DEFINED TO RACF

Explanation: The indicated name (user ID or group name) is not defined to RACF and cannot be granted access to the resource.

System action: Command processing continues with the next name specified on the command.

ICH06008I INSTALLATION EXIT FAILED PERMIT REQUEST FOR profile-name

Explanation: The command preprocessing exit routine ICHCNX00 issued a return code of 4, indicating that RACF should fail the permit request for the profile indicated in the message.

System action: If the command attempted to modify the access list of the profile, command processing stops. If the command attempted to copy the access list of the
profile specified on the FROM operand, only the processing associated with the ID operand is performed.

**User response:** Report this message to your system programmer.

**ICH06009I**  
**RESET OPTION IGNORED, CONFLICTS WITH DELETE REQUEST**

**Explanation:** Both the DELETE and the RESET options were specified.

**System action:** RACF accepts the DELETE option and ignores the RESET option.

**ICH06010I**  
**{GENERIC | FGENERIC} INVALID, GENERIC COMMAND PROCESSING IS INACTIVE.**

**Explanation:** Because the generic command processing facility is inactive, the GENERIC and FGENERIC operands are not valid.

**System action:** Command processing stops.

**ICH06011I**  
**RACLISTED PROFILES FOR class-name WILL NOT REFLECT THE UPDATE(S) UNTIL A SETROPTS REFRESH IS ISSUED**

**Explanation:** The changes to the profiles do not become effective until the SETROPTS command is issued with the REFRESH and RAelist operands. This message can be ignored if the following conditions are true:

- It results from processing the RALTER command for a STARTED or DLFCCLASS profile.
- The command only changed data in the STDATA or DLFDATA segments.

**System action:** RACF updates the profiles in the RACF database, but does not update the in-storage copies of the profiles.

**ICH06013I**  
**WHEN(class-name(*)) OPERAND IGNORED. INVALID WITH ACCESS OPERAND.**

**Explanation:** A PERMIT command was issued with both the ACCESS and WHEN(class-name(*)) operands specified. WHEN(class-name(*)) is valid only when specified with the DELETE operand.

**System action:** Command processing stops.

**ICH06014I**  
**userid not authorized, DELETE ignored for WHEN(class-name(resource-name))**

**Explanation:** The user issued the PERMIT command with the DELETE and WHEN keywords specified. The class name and resource name specified on the WHEN keyword are indicated in the message. This attempted to delete an entry from the conditional access list. However, the entry was not found.

**System action:** Command processing continues with the next DELETE request.

**User response:** Check the spelling of the values specified for the ID, ACCESS, and WHEN operands, and reissue the command. To check the profile itself, enter the RLIST command with AUTHUSER specified.

**ICH06015I**  
**WARNING - In class class-name resource resource-name not currently protected by RACF.**

**Explanation:** The PERMIT command was issued with the WHEN operand specified for the indicated class. However, the indicated resource is not protected by a profile in the class.

**Note:** When using WHEN(SERVAUTH), the resource-name must be the name of a profile, not a name protected by a profile.

**System action:** The entry is added to the conditional access list and used by RACF when appropriate.

**User response:** Ensure that the resource name specified in the WHEN operand was spelled correctly. If it was not, use the PERMIT command to delete this conditional access list entry and then create the correct entry. If the resource name is spelled correctly and you believe it should be protected by RACF, examine the profiles in the class specified in the WHEN operand to determine why the resource is not considered protected by RACF.

**ICH06016I**  
**Access unchanged. userid already has access defined by WHEN(class-name(resource-name)).**

**Explanation:** The user indicated in the message is already on the conditional access list with the access specified.

**System action:** The conditional access list is not changed.

**ICH06017I**  
**WARNING for command-name. Extraneous information in the FROM keyword has been ignored.**

**Explanation:** For the PERMIT command, only one profile name (no blanks) is allowed in the FROM operand.

**System action:** The first profile name (no blanks) in the FROM operand is used, and the other names are ignored.

**User response:** If the access list was modified using the wrong FROM profile, delete the incorrect access list entries that were created and issue the command again.
ICH06018I  command-name failed. WHEN operand is incorrect without a value.

Explanation:  The user did not specify a keyword for the WHEN operand. Valid keywords are PROGRAM, JESINPUT, CONSOLE, APPCPORT, SERVAUTH, SYSID, TERMINAL, or CRITERIA(SQLROLE(...)).

System action:  Command processing stops.

ICH06019I  WARNING: Class class-name is not currently active.

Explanation:  The PERMIT command was issued with the WHEN operand specified for the indicated class. However, the indicated class is not active.

System action:  The entry is added to the conditional access list, but it has no effect until the class is activated by the SETROPTS CLASSACT (class-name) command.

ICH06020I  command-name failed. WHEN(PROGRAM) operand is invalid for this class.

Explanation:  The WHEN(PROGRAM) operand is only valid for the DATASET class or SERVAUTH class.

System action:  RACF stops processing the command.

ICH06021I  command-name FAILED. WHEN(SYSID) IS NOT VALID FOR THIS CLASS.

Explanation:  The WHEN(SYSID) operand is only valid for the PROGRAM class.

System action:  RACF stops processing the command.

ICH06022I  PERMIT FAILED. WHEN(CRITERIA) IS NOT VALID FOR THIS CLASS.

Explanation:  The WHEN(CRITERIA) operand is only valid for general resource classes.

System action:  RACF stops processing the command.

ICH06023I  PERMIT failed. The criteria-value cannot end with a blank.

Explanation:  The quoted string specified as the criteria-value contained trailing blanks. Criteria values cannot end with a blank.

System action:  RACF stops processing the command.

RACF Security Administrator Response:  Remove the trailing blanks and reissue the command.
**PASSWORD command messages**

**ICH08001I**  
**userid NOT DEFINED TO RACF**  
Explanation: The indicated user ID was not found in the RACF database.  
System action: No processing is done.

**ICH08002I**  
**NEW PASSWORD CANNOT EQUAL CURRENT PASSWORD**  
Explanation: The new password specified must be different from the current password.  
System action: The password is not changed.

**ICH08003I**  
**INTERVAL NOT IN RANGE 1-nnn**  
Explanation: The password change-interval must be greater than 0 and less than nnn, which is the installation-specified maximum.  
System action: The interval is not changed.

**ICH08004I**  
**COMMAND ENDED DUE TO ERROR**  
Explanation: A RACF manager error occurred. This message is accompanied by a message explaining the error.

**ICH08005I**  
**VALUE SPECIFIED IS NOT CURRENT PASSWORD**  
Explanation: The value specified for the current password is not correct.  
System action: The password is not changed.

**ICH08006I**  
**NOT AUTHORIZED TO ISSUE (PASSWORD | PHRASE)**  
Explanation: You attempted to issue the indicated PASSWORD or PHRASE command and one of the following conditions is true:  
- RACF is inactive.  
- You are not defined to RACF and cannot issue RACF commands.  
- You are not defined to RACF with sufficient authority to issue this command.  
System action: Command processing stops.  
User response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.  
RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or the authority required to issue the indicated command, see z/OS Security Server RACF Command Language Reference.

**ICH08007I**  
**NOT AUTHORIZED TO CHANGE PASSWORD/INTERVAL FOR userid**  
Explanation: You are not allowed to change the password or password interval for the user indicated in the message.  
System action: The password is not changed.  
User response: See your RACF security administrator.

**ICH08008I**  
**userid NOT DEFINED TO USE A PASSWORD**  
Explanation: The indicated user ID is defined to RACF but does not require a password to enter the system.  
System action: No command processing is performed.

**ICH08009I**  
**PASSWORD OPERAND IGNORED**  
Explanation: You specified the PASSWORD operand with the USER operand.  
System action: Only the USER operand is processed. The PASSWORD operand is ignored.

**ICH08010I**  
**INTERVAL CHANGE FOR ‘id’ REJECTED BY**  
Explanation: This is the first part of a two-part message that indicates that the installation password exit (ICHPWX01) has rejected the value you specified in the INTERVAL keyword (in the PASSWORD command). Message ICH08012I completes this message.  
System action: Command processing stops.  
User response: See your RACF security administrator for the rules for interval values.

**ICH08011I**  
**PASSWORD CHANGE FOR ‘id’ REJECTED BY**  
Explanation: This is the first part of a two-part message indicating that the installation password exit (ICHPWX01) has rejected the character string you specified in the PASSWORD operand (on the PASSWORD command). Message ICH08012I follows this message.  
System action: Command processing stops.  
User response: See your RACF security administrator for the rules regarding new passwords.
ICH08012I • INSTALLATION PASSWORD EXIT

Explanation: This message completes messages ICH08010I, ICH08111I and ICH08013I.

ICH08013I • PASSWORD AND INTERVAL CHANGES FOR id REJECTED BY

Explanation: This is the first of a two-part message that indicates that the installation password exit (ICHPWX01) has rejected the values you specified in both the INTERVAL and PASSWORD operands (on the PASSWORD command).

Message ICH08012I follows this message.

System action: Command processing stops.

User response: See your RACF security administrator for the rules for interval values and new passwords.

ICH08014I • PASSWORD CHANGE REJECTED BY INSTALLATION SYNTAX RULES

Explanation: You specified a potential password that does not adhere to the syntax rules that are in effect for your installation.

System action: Command processing stops.

User response: See your RACF security administrator for the syntax rules for passwords.

ICH08015I • NEW PASSWORD MATCHES A PREVIOUS PASSWORD FOR YOU

Explanation: You specified a password that matches a previous password. Your system restricts the use of previously used passwords.

System action: Command processing stops.

User response: See your RACF security administrator for password HISTORY options set by the SETROPTS command.

ICH08016I • ERROR SETTING KERBEROS KEY INFORMATION

Explanation: An error occurred while attempting to generate a Kerberos key for the user changing their own password with the PASSWORD command.

System action: All processing except for the key update is completed.

User response: Report this message to the system programmer and provide the exact text of the command issued.

System programmer response: Use the RLIST command to list the KERBDFLT profile definition of the local Kerberos realm in the REALM class and verify that the local realm name (KERBNAME) is defined. Use the LISTUSER command to list the KERB segment information for this user and verify that this information may be accessed. Correct any problem and ask the user to reissue the command.

ICH08017I • PASSWORD CHANGE REJECTED DUE TO INSTALLATION MINIMUM CHANGE INTERVAL

Explanation: The PASSWORD command has detected that an insufficient number of days has passed since your last password change.

System action: RACF ignores the operand and continues command processing with the next operand.

User response: Contact your security administrator to determine your installation's minimum password change interval, and to reset your password if it has been compromised.

ICH08018I • PASS PHRASE CHANGE REJECTED DUE TO INSTALLATION MINIMUM CHANGE INTERVAL

Explanation: The PASSWORD command has detected that an insufficient number of days has passed since your last password phrase change.

System action: RACF ignores the operand and continues command processing with the next operand.

User response: Contact your security administrator to determine your installation's minimum password change interval because it also applies to password phrases, and reset your password phrase if it has been compromised.

ICH08019I • PASS PHRASE CHANGE REJECTED BY INSTALLATION PASS PHRASE EXIT

Explanation: The proposed password phrase, as specified in the PHRASE operand on the PASSWORD command, has been rejected by the installation password phrase exit, ICHPWX11.

System action: RACF ignores the operand and continues command processing with the next operand.

User response: See your RACF security administrator for the rules regarding new password phrases.

ICH08020I • NEW PASS PHRASE REJECTED BY RACF RULES

Explanation: You specified a potential password phrase that does not adhere to the following syntax rules:

- The user ID is not part of the password phrase.
- At least 2 alphabatics are specified (A - Z, a - z).
- At least 2 non-alphabetics are specified (numerics, punctuation, special characters).
No more than 2 consecutive characters are identical.

**System action:** RACF ignores the operand and continues command processing with the next operand.

**User response:** Try again with a different password phrase.

**ICH08021I NEW PASS PHRASE CANNOT EQUAL CURRENT PASS PHRASE**

**Explanation:** The new password phrase specified must be different from the current password phrase.

**System action:** The password phrase is not changed.

**ICH08022I VALUE SPECIFIED IS NOT CURRENT PASS PHRASE**

**Explanation:** The value specified for the current password phrase is not correct, or there is no current password phrase assigned.

**System action:** The password phrase is not changed.

**ICH08023I PHRASE OPERAND IGNORED**

**Explanation:** You specified the PHRASE operand with the USER operand.

**System action:** Only the USER operand is processed. The PHRASE operand is ignored.

**ICH08024I NEW PASS PHRASE CANNOT MATCH A PREVIOUSLY USED PASS PHRASE**

**Explanation:** You specified a password phrase that matches a previous password phrase. Your system restricts the reuse of password phrases.

**System action:** The password phrase is not changed.

**User response:** See your RACF security administrator for password HISTORY options set by the SETROPTS command because this also applies to password phrases.
ADDSD and DELDSD command messages

ICH09000I  NOT AUTHORIZED TO ISSUE command-name
Explanation: One of the following conditions is true:
• RACF is inactive.
• You are not defined to RACF and cannot issue RACF commands.
• You are not defined to RACF with sufficient authority to issue this command.
System action: Command processing stops.
User response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or the authority required to issue the indicated command, see z/OS Security Server RACF Command Language Reference.

ICH09001I  UNABLE TO ESTABLISH ESTAE
Explanation: The command processor was unable to establish an ESTAE recovery environment.
System action: Command processing stops.
User response: Report this message to your system programmer. Include the following information:
• The message ID
• The exact wording of the command you entered
• The date and time you entered the command.
System programmer response: Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

ICH09002I  NOT AUTHORIZED TO CREATE GROUP DATASETS FOR GROUP group-name
Explanation: You do not have sufficient authority to create group data sets. Processing continues with the next data set.
User response: See your RACF security administrator or the group administrator for the group indicated in the message.

ICH09004I  profile-name ALREADY DEFINED TO RACF
Explanation: The data set name indicated in the message was found in the RACF database.

ICH09005I  dsname NOT FOUND [ON volume | IN CATALOG]
Explanation: If “ON volume” appears in the message, the specified non-VSAM data set name was not found on the indicated volume.
If “IN CATALOG” appears in the message, the specified VSAM or non-VSAM data set name was not found by a catalog search.
System action: If the data set was not found on a particular volume, the command processor attempts to process the data set on any remaining volumes.
If the data set cannot be found in the catalog, processing continues with the next data set.

ICH09006I  USER OR GROUP name NOT DEFINED TO RACF
Explanation: The indicated name (user ID or group name) was specified as the first-level qualifier of the data set name but cannot be found on the RACF database. To protect a data set with RACF, the first-level qualifier of the data set name must be a RACF-defined user ID or group name.
System action: Processing continues with the next data set.

ICH09007I  OWNER SPECIFIED IS NOT A RACF DEFINED USER OR GROUP
Explanation: The user ID or group name specified on the OWNER operand is not defined to RACF.
System action: Command processing stops.

ICH09008I  VOLUME INFORMATION IN RACF PROFILE INCONSISTENT WITH CATALOG VOLUME INFORMATION
Explanation: In processing a request to delete RACF protection for a VSAM data set, RACF found that the volume serial number in the data set profile does not match the volume serial number in the containing catalog.
System action: Command processing stops.
Problem Determination: Use the Access Method Services LISTCAT command and the RACF LISTDSD command to locate the inconsistency. Processing continues with the next data set.
ICH09009I OWNER SPECIFIED HAS INSUFFICIENT AUTHORITY TO GROUP

Explanation: For a group data set, the user ID specified on the OWNER operand does not have group authority to the group and cannot be named the owner of the group data set.

System action: Command processing stops.

User response: See your RACF security administrator.

ICH09010I NOT AUTHORIZED TO SPECIFY NOSET

Explanation: To specify NOSET, one of the following conditions must be true:

- Your user ID must match the first-level qualifier of the data set name.
- You must have the SPECIAL attribute.
- The data set profile is within the scope of a group in which you have the group-SPECIAL attribute.

System action: Processing continues with the next data set.

ICH09011I NOT AUTHORIZED TO DELETE RACF PROTECTION FOR dsname

Explanation: You do not have sufficient access authority to delete RACF protection for the data set specified.

System action: Processing continues with the next data set.

User response: See your RACF security administrator.

ICH09012I dsname [ON volume] ALREADY RACF INDICATED

Explanation: While attempting to RACF-indicate the data set named in the message, the command processor found that the data set was already RACF-indicated. For a VSAM data set, the RACF indicator is in the VSAM catalog. For a non-VSAM DASD data set, the RACF indicator is in the DSCB on the volume indicated in the message. For a tape data set, the RACF indicator is in the TVTOC for the tape volume indicated in the message.

System action: Processing continues with the next data set.

ICH09013I dsname [ON volume] IS NOT RACF INDICATED

Explanation: While attempting to remove RACF indication for the data set named in the message, the command processor found that the data set was not RACF-indicated. The RACF indicator is in the VSAM catalog for a VSAM DASD data set, in the DSCB on the indicated volume for a non-VSAM DASD data set, or in the TVTOC for tape volume volume.

System action: Processing continues with the next data set.

ICH09014I INCOMPLETE UNIT/VOLUME INFORMATION SPECIFIED

Explanation: Either unit or volume information was specified, but not both. If the data set is cataloged, do not specify unit or volume. If the data set is not cataloged, specify both unit and volume.

System action: Command processing stops.

ICH09015I I/O ERROR ON OBTAIN ON VOLUME volume

Explanation: An OBTAIN issued for the data set on the volume indicated resulted in an error return code.

System action: Command processing stops.

ICH09016I VSAM CATALOG RETURN CODE IS rc - REASON CODE IS IGGOCLaa - crs

Explanation: The return code rc and reason code crs were returned by the catalog management module IGGOCLaa as a result of a catalog error or exceptional condition. For an explanation of the return and reason codes, see the description of message IDC3009I in the system messages documentation for your system.

System action: Processing continues with the next data set.

ICH09017I I/O ERROR PROCESSING VTOC ON VOLUME volume

Explanation: An I/O error occurred while reading or writing a DSCB to the volume indicated.

System action: Command processing stops.

ICH09018I OPEN FAILED ON VOLUME volume

Explanation: An OPEN failed for the data set to be protected or for the VTOC data set on the volume indicated.

System action: Command processing stops.

ICH09019I dsname [ON volume] - RACF INDICATOR INCONSISTENT WITH DATA SET PROFILE

Explanation: RACF protection was partially added or deleted for the data set indicated in the message.

System action: The RACF indicator for the data set was processed successfully in the VSAM catalog entry, in the DSCB on DASD volume volume, or in the TVTOC for tape volume volume, but the associated data
set profile on the RACF database was not successfully processed. Processing continues with the next data set.

ICH09020I  profile-name NOT DEFINED TO RACF
Explanation: The profile in the message was not found on the RACF database.

Note: If you enter the DELDSD command for a fully qualified generic profile (one whose name has no generic characters), but you do not specify the GENERIC operand, RACF issues this message. This occurs because, without the GENERIC operand, RACF looks for a discrete profile of that name. For example, if there is a fully qualified generic profile named ABC.DATA, and you enter the following command:

DELDSD 'ABC.DATA'

RACF looks for a discrete profile named ABC.DATA and, if there is none, issues this message (ICH09020I ABC.DATA NOT DEFINED TO RACF). To identify for RACF the generic profile, specify the GENERIC operand as follows:

DELDSD 'ABC.DATA' GENERIC

System action: Processing continues with the next profile name.

ICH09021I  dsname [ON volume] [AND REMAINING VOLUMES] NOT PROCESSED
Explanation: RACF processing was not successful for the indicated data set. For non-VSAM data sets, RACF processing was not successful on the volume volume. The phrase “AND REMAINING VOLUMES” means that all volumes sequentially after the indicated volume in the catalog entry for the data set or in the VOL list specified on the command were not processed.

ICH09022I  COMMAND PROCESSOR ENCOUNTERED SYSTEM ERROR
Explanation: The RDJFCB function failed during the processing of the RACF indicator for a volume of a non-VSAM data set.

System action: Command processing stops.

ICH09023I  profile-name - LAST VOLUME ADDED TO DATA SET PROFILE WAS volume
Explanation: During processing of the ADDSD command with the NOSET operand specified, an error occurred while adding volume serials to the newly created data set profile on the RACF database. The volume volume was the last volume added before the error occurred.

System action: Command processing stops.
User response: Use the ADDVOL operand of the ALTDSD command to add the remaining volumes.

ICH09024I  dsname INVALID DATA SET NAME
Explanation: The data set indicated in the message is not a valid qualified name or the first qualifier exceeded the maximum allowed length of 8 characters.

System action: Command processing stops.

ICH09025I NOT AUTHORIZED TO RACF PROTECT dsname
Explanation: You are not authorized to RACF-protect the data set indicated in the message.

System action: Command processing stops.
User response: See your RACF security administrator.

ICH09026I  dsname HAS DUPLICATE VOLUME SERIALS
Explanation: The same volume serial was found twice in the list of volume serials for the data set indicated in the message.

System action: RACF does not process any volumes and stops processing the command.

ICH09027I  dsname IN USE - TRY AGAIN LATER
Explanation: For the VSAM data set indicated in the message, the catalog entry containing the RACF indicator cannot be modified because the data set is in use.

System action: Processing continues with the next data set.

ICH09028I INSTALLATION EXIT FAILED
Explanation: The command preprocessing exit routine ICHCNX00 issued a return code of 4, indicating that RACF should fail the ADDSD or DELDSD request for the profile indicated in the message.

System action: Command processing stops.
User response: Report this message to your system programmer.

ICH09029I ERROR ENCOUNTERED DURING VTOC PROCESSING, RETURN CODE IS xx, CVSTAT IS yyy.
Explanation: The Common VTOC Access Facility (CVAF) issued a return code other than zero, indicating that a VTOC update operation was not completed successfully.
User response: Report the exact text of this message to your system programmer.

System programmer response: See “Problem Determination.”

Problem Determination: Return code xx (the contents of register 15 from a CVAF invocation) and CVSTAT value yyy are documented in MVS/ESA Common VTOC Access Facility Diagnosis Reference and z/OS DFSMSdfp Diagnosis.

ICH09030I  FILESEQ(mmmn) ALREADY DEFINED IN TVTOC FOR SPECIFIED VOLUME(S)

Explanation: For a tape data set, file sequence number mmmn is already defined in the TVTOC for the volume(s) specified. Message ICH09021I will follow this message.

System action: Command processing continues with the next data set.

ICH09031I  COMMAND PROCESSING TERMINATED. FILESEQ(mmmn) IS INCONSISTENT WITH CURRENT VOLUME CONTENTS

Explanation: The specified tape volumes already have data sets defined, and the file sequence number mmmn would fall after a multivolume data set on the first volume specified, or the second or remaining volumes are not currently empty, or the specified tape volume has been marked as a single data set volume and the file sequence number specified is greater than one.

System action: Command processing stops.

ICH09032I  UNABLE TO LOCATE TAPE VOLUME FOR DATA SET

Explanation: A specific volume for the data set was not specified. RACF attempted to locate a catalog entry for the tape data set and an entry cannot be found.

System action: Command processing stops.

User response: Specify the correct volume for the data set.

ICH09033I  TAPE DATA SET PROTECTION IS INACTIVE. TAPE IS NOT VALID

Explanation: The TAPE operand may not be specified because tape data set protection is inactive.

System action: Command processing stops.

User response: See your RACF security administrator for information on protecting tape data sets.

ICH09034I  GENERIC INVALID, GENERIC COMMAND PROCESSING IS INACTIVE

Explanation: The GENERIC operand is not valid because the generic command processing facility is inactive.

System action: Command processing stops.

ICH09035I  COMMAND PROCESSING TERMINATED. USER NOT AUTHORIZED TO ‘FROM’ PROFILE profile-name

Explanation: The user does not have sufficient authority to the profile specified in the FROM operand.

System action: Command processing stops.

User response: See your RACF security administrator.

ICH09036I  COMMAND PROCESSING TERMINATED. ‘FROM’ PROFILE profile-name DOES NOT EXIST

Explanation: The profile name specified in the FROM operand is not an existing profile.

If the FVOLUME operand was specified, RACF cannot locate a profile with the specified name and volume.

If the FVOLUME operand was not specified, one of the following conditions is true:

• There is no profile with the specified name.
• There is more than one discrete profile with the same name protecting data sets on different volumes.

Note: For fully qualified generic names, the FGENERIC operand must be specified in order to find a matching generic profile.

System action: Command processing stops.

ICH09037I  NOT AUTHORIZED TO USE VOLUME mmmn

Explanation: The tape volume is already RACF-protected and the current user has insufficient authority to it.

System action: Command processing stops.

User response: Check the spelling of the volume on the command issued. If it is correct, see your RACF security administrator to obtain the appropriate authority.

ICH09038I  COMMAND PROCESSING TERMINATED. USER SPECIFIED FOR NOTIFY NOT RACF DEFINED

Explanation: The user ID specified on the NOTIFY operand is not a RACF-defined user.
ICH09039I  COMMAND PROCESSING Terminated. Multiple Tape Data Sets and Multiple Volumes Were Specified

Explanation: The user has specified multiple tape data sets and multiple volumes. Either multiple tape data sets or multiple volumes may be specified, but not both.

System action: Command processing stops.

ICH09041I  COMMAND PROCESSING Terminated. FGENERIC Not Authorized for FCLASS Specified

Explanation: FGENERIC was specified, but the class indicated by FCLASS does not have generic profile checking or generic profile command processing active.

System action: RACF stops processing the command.

ICH09042I  COMMAND PROCESSING Terminated. No SECLEVELS | CATEGORIES Found

Explanation: RACF cannot validate the name you specified on the SECLEVEL or ADDCATEGORY operand. This happened for one of two reasons:

- There is no SECLEVEL or CATEGORY profile.
- A profile is defined, but it does not contain any members.

System action: RACF stops processing the command.

ICH09043I  COMMAND PROCESSING Terminated. TapeVol Profile Profile-name Cannot Contain a TVTOC.

Explanation: Profile profile-name was defined without a TVTOC. ADDSD command cannot be used.

System action: RACF stops processing the command.

User response: Contact your RACF security administrator.

ICH09044I  NOT AUTHORIZED TO INCLUDE DFP SEGMENT IN DATASET PROFILE DSNNAME DATASET PROFILE WAS NOT DEFINED

Explanation: The ADDSD command with RESOWNER operand specified was issued by a user without sufficient authority.

System action: Command processing stops without adding a data set profile to the RACF database.

User response: See your RACF security administrator.

ICH09045I  ADDSD failed. You are not authorized to specify SECLABEL.

Explanation: The security label operand was specified on the ADDSD command, but the user does not have the SPECIAL attribute and SETROPTS SECLABELCONTROL is in effect.

System action: Command processing stops.

User response: See your RACF security administrator.

ICH09046I  DELDSD failed. There is a less specific profile profile-name with a different SECLABEL.

Explanation: The SETROPTS MLSTABLE option is in effect. Therefore, the execution of the particular DELDSD command can potentially change the security label of the data set, because of the existence of a less specific profile with a different security label.

System action: Command processing stops.

User response: See your RACF security administrator.

ICH09047I  ADDSD failed. There is a less specific profile profile-name with a different SECLABEL.

Explanation: The SETROPTS MLSTABLE option is in effect, but SETROPTS MLQUIET is not in effect. Therefore, the execution of the particular ADDSD command can potentially change the security label of the data set, because of the existence of a less specific profile with a different security label.

System action: Command processing stops.

User response: See your RACF security administrator.

ICH09048I  Your current SECLABEL seclabel-name has been used. FROM profile has a different SECLABEL.

Explanation: The ADDSD command was issued with FROM specified, but the FROM profile has a different security label than the profile being defined, and the SETROPTS options prevent security label changes by a user without the appropriate authority. One of the following conditions is true:

- The user did not have the SPECIAL attribute, and SETROPTS SECLABELCONTROL was in effect.
- SETROPTS MLSTABLE was in effect, but SETROPTS MLQUIET was not in effect.

RACF Security Administrator Response: You can use field-level access checking to allow this user to add DFP segment information. For a description of field-level access checking, see z/OS Security Server RACF Security Administrator's Guide.
System action: The command executes but the security label is not copied from the model profile. The current security label of the issuer is used.

ICH09049I ADDSD failed. SECLABEL seclabel-name is not currently defined to RACF.

Explanation: There is no profile in class SECLABEL whose name is the security label indicated in the message.

System action: Command processing stops.
User response: Check the spelling of the value specified on the security label operand. If it is correct, report the exact text of this message to your RACF security administrator.

ICH09050I RACDEF FAILED. RETURN CODE IS return-code, REASON CODE IS reason-code

Explanation: RACROUTE REQUEST=DEFINE failed for one of the following reasons:
- There is an error in an installation exit.
- An installation exit (such as ICHRDX01) returned a return code of 4.
- There is an internal error.

System action: Command processing stops.
User response: See your RACF security administrator.

Problem Determination: See the description of return and reason codes for the REQUEST=DEFINE macro in z/OS Security Server RACROUTE Macro Reference. Check any related installation exit for a possible error.

ICH09051I ADDSD failed. You are not authorized to specify SECLABEL seclabel-name.

Explanation: To specify the security label indicated in the message, you must have at least READ access authority to the security label profile.

System action: Command processing stops.
User response: See your RACF security administrator.

ICH09052I ADDSD failed. SECLABEL is required under the current RACF options.

Explanation: The SETROPTS MLACTIVE option is in effect on your system, which requires that all new profiles have a security label specified. However, the security label operand was not specified on the ADDSD command, and you have no current security label.

System action: Command processing stops.
User response: Specify a security label appropriate for the profile. For a description of available security labels, see your installation security procedures or your RACF security administrator.

ICH09053I Profile not deleted. This profile is the only profile providing SECLABEL protection for one or more data sets.

Explanation: You cannot delete the profile specified on the DELDSD command because it is the only remaining profile that protects one or more data sets with a security label, and the SETROPTS MLACTIVE option prevents changes to security label protection.

System action: Command processing stops with no effect on profiles.
User response: Check the spelling of the command you entered. If it is correct and you intend to delete this profile, rename or delete all data sets protected by the profile, then reissue the DELDSD command.

ICH09054I CATALOG NOT available. Data set, dsname, was not processed.

Explanation: The device containing the catalog has been dynamically reconfigured from the system.

System action: Processing continues with the next data set.
User response: Report this message to your system programmer.

System programmer response: Before this data set can be processed, the device containing the catalog must be dynamically re-configured back into the system.

ICH09059I MODEL parameter not valid with GENERIC profile. Parameter ignored.

Explanation: Profile names containing generic characters imply that the profile is generic. Generic profiles created with the ADDSD command cannot have a data set type of MODEL, because the MODEL and GENERIC keywords are mutually exclusive.

System action: The MODEL keyword is ignored and the profile is added with a data set type of NON-VSAM.
RDEFINE command messages

ICH10004I operand DOES NOT APPLY TO class-name CLASS ENTITIES; OPERAND IGNORED

Explanation: The operand indicated in the message does not apply to the class indicated in the message.
System action: RACF ignores the operand and continues processing with the next operand.

ICH10005I LIST OF ENTITY NAMES SPECIFIED; ADDMEM OPERAND IGNORED

Explanation: The RDEFINE command was issued with a list of entity names (profile names), a class name of GLOBAL or SECDATA, and the ADDMEM operand. Only a single entity name (profile name) is allowed.
System action: RACF ignores the ADDMEM operand. Command processing continues with the next operand.

ICH10006I THE NEW PROFILE WILL NOT BE IN EFFECT UNTIL A SETROPTS REFRESH HAS BEEN ISSUED.

Explanation: The profile class exists in common storage, but the new profile does not become effective until the SETROPTS command is issued with the REFRESH operand.

ICH10102I profile-name ALREADY DEFINED TO class-name

Explanation: The indicated profile has been previously defined to RACF in the indicated class.
System action: Command processing continues with the next profile name.

ICH10103I NOT AUTHORIZED TO DEFINE profile-name

Explanation: You do not have sufficient authority to define the indicated profile to RACF.
System action: Command processing continues with the next profile name in the list.
User response: See your RACF security administrator.

ICH10104I NOT AUTHORIZED TO ADD member-name

Explanation: You do not have sufficient authority to specify the indicated resource name on the ADDMEM operand.
System action: Command processing continues with the next member name.
User response: See your RACF security administrator.

ICH10105I LEADING ZEROES ARE NOT ALLOWED WHEN DEFINING FOUR CHARACTER MINIDISK. profile-name IS NOT DEFINED.

Explanation: When specifying the profile names for minidisks that have four character virtual addresses, you cannot specify a zero as the first character in the virtual address. You must omit the leading zero. For example, for SMITH's 0191 minidisk, specify the following profile name:
SMITH.191

System action: Command processing continues with the next profile name.
User response: Change the spelling of the profile name and issue the command again.

ICH10201I NOT AUTHORIZED TO ISSUE command-name

Explanation: One of the following conditions is true:
- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.
System action: Command processing stops.
User response: If RACF is inactive, log on when RACF is active or contact your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the user to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or about the authority required to issue the indicated command see z/OS Security Server RACF Command Language Reference.

ICH10202I NOT AUTHORIZED TO DEFINE class-name CLASS ENTITIES

Explanation: You do not have sufficient authority to define entities (profiles) to RACF in the indicated class.
System action: Command processing stops.
User response: See your RACF security administrator.

ICH10203I COMMAND PROCESSING TERMINATED. NOT AUTHORIZED TO ‘FROM’ PROFILE profile-name.

Explanation: The user does not have sufficient authority to the profile specified in the FROM operand.
ICH10204I  COMMAND PROCESSING TERMINATED. ‘FROM’ PROFILE profile-name NOT FOUND

Explanation: The profile name specified in the FROM operand is not an existing profile.

If the FVOLUME operand was specified, RACF cannot locate a profile with the specified name and volume.

If the FVOLUME operand was not specified, one of the following conditions is true:

• There is no profile with the specified name.
• If FCLASS is DATASET, there is more than one discrete profile with the same name protecting data sets on different volumes.

Note: For fully qualified generic names with FCLASS(DATASET), the FGENERIC operand must be specified in order to find a matching generic profile.

System action: Command processing stops.

ICH10207I  COMMAND PROCESSING TERMINATED. NO {SECLEVEL | CATEGORIES} FOUND

Explanation: RACF cannot validate the name you specified on the SECLEVEL or ADDCATEGORY keyword. This happened for one of two reasons:

• There is no SECLEVEL or CATEGORY profile.
• A profile is defined, but it contains no members.

System action: Command processing stops.

ICH10301I  entity-name AND REMAINING ENTITIES NOT DEFINED TO RACF

Explanation: The indicated entity name (profile name) and remaining entity names in the list were not defined to RACF because of one of the following reasons:

• A user attempted to define (through RDEFINE) a profile containing generic characters in a class that did not have SETROPTS GENERICs active and also specified the FROM keyword containing a profile in a class that did have SETROPTS GENERICs active.
• A RACF manager error occurred. In this case, a RACF manager error message explaining the error precedes this message.
• A system error occurred while building in-storage profiles (using RACROUTE REQUEST=LIST) for the indicated entity name.
• A system error occurred while checking (with REQUEST=FASTAUTH) the user’s authority to the entities to be defined.

• A system error occurred while building in-storage profiles (using REQUEST=LIST) for the entity names specified by the ADDMEM operand, or the member class associated with the specified class is currently inactive.
• A system error occurred while checking (with REQUEST=FASTAUTH) the user’s authority to the entities specified by the ADDMEM operand.
• A user with class authority (CLAUTH) but without the SPECIAL attribute attempted to define an entity in a general resource class (for example, TIMS) while the class was not active.

ICH10302I  NOT AUTHORIZED TO ADD member-name WITH THE OPTION SPECIFIED.

Explanation: The user has attempted to add a member to a VMEVENT or VMXEVENT class profile and has specified an auditing or control option without the correct authority.

System action: RACF stops processing the command.

User response: See your RACF security administrator.

ICH10303I  command-name failed. You are not authorized to specify SECLABEL.

Explanation: The command indicated in the message was issued with the security label operand. However, one of the following conditions caused the command to fail:

• The user issuing the command did not have the SPECIAL attribute, and SETROPTS SECLABELCONTROL is on.
• The security label operand was specified on the RDEFINE command, and SETROPTS MLSTABLE is on, but SETROPTS MLQUIET is not.

System action: Command processing stops.

User response: See your RACF security administrator.

ICH10304I  command-name failed. There is a less specific profile profile-name with a different SECLABEL.

Explanation: The execution of the command indicated in the message can potentially change the security label of the resource because of the existence of a less specific profile with a different security label.

System action: Command processing stops.

User response: See your RACF security administrator.
ICH10305I  Your current SECLABEL seclabel-name was used. FROM profile has a different SECLABEL.
Explanation:  RDEFINE FROM was issued, but the FROM profile has a different security label, and the SETROPTS options preventing the security label change by a user without the appropriate authority have been turned on.
System action:  The command executes, but the security label is not copied from the model profile. The LOGON SECLABEL of the issuer is used.
User response:  If the profile was created by using the wrong FROM profile, delete the profile that was created and create it again.

ICH10306I  command-name failed. SECLABEL seclabel-name is not currently defined to RACF.
Explanation:  There is no profile in class SECLABEL whose name is the security label indicated in the message.
System action:  Command processing stops.
User response:  Correct the command or define the security label.

ICH10307I  SECLABEL operand ignored. It does not apply to class class-name.
Explanation:  The security label operand was specified on the command, but security label has no meaning for the class. The operand has been ignored by the command processor.
System action:  The profile is defined, but the security label operand is ignored.
User response:  If the profile was created by using the wrong FROM profile, delete the profile that was created and create it again.

ICH10308I  command-name failed. You are not authorized to specify SECLABEL seclabel-name.
Explanation:  SECLABEL seclabel-name was specified on the command indicated in the message by a user without at least READ authority to it.
System action:  Command processing stops.
User response:  See your RACF security administrator.

ICH10309I  WARNING for command-name. Extrinsic information in the FROM keyword has been ignored.
Explanation:  For the RDEFINE command, only one profile name (no blanks) is allowed in the FROM operand.
System action:  The first profile name (no blanks) in the FROM operand is used. Any characters that follow the first blank are ignored.
User response:  If the profile was created by using the wrong FROM profile, delete the profile that was created and create it again.

ICH10310I  command-name failed. User userid is not defined to RACF.
Explanation:  The user ID indicated in the message was specified as the second qualifier in a file profile name but cannot be found in the RACF database. The second qualifier in the profile name for a file must be a RACF-defined user ID.
System action:  Command processing stops.
User response:  Correct the second qualifier in the profile name and issue the command again.

ICH10311I  command-name failed. SECLABEL is required under the current RACF options.
Explanation:  The SETROPTS MLACTIVE option is in effect on your system, which requires that all new profiles have a security label specified. However, the security label operand was not specified on the indicated command, and you have no current security label.
System action:  Command processing stops.
User response:  Specify a security label appropriate for the profile. For a description of available security labels, see your installation security procedures or your RACF security administrator.

ICH10312I  Profile not created. You must specify the SECLEVEL keyword when creating a SECLABEL profile.
Explanation:  The user attempted to create a security label profile without specifying a security level. Each security label profile must have a security level.
System action:  The security label profile is not created.
User response:  After choosing an appropriate security level for this security label, specify it on the SECLEVEL keyword.

ICH10313I  Profile cannot be defined. Profile names cannot end with ‘%*’.
Explanation:  The user of the RDEFINE command attempted to define a profile ending with ‘%*’.
System action:  Command processing stops.

ICH10315I  PROFILES ARE NOT ALLOWED TO BE ADDED TO CLASS class-name.
Explanation:  The user of the RDEFINE command attempted to define a profile to a class that has been
defined in the class descriptor table with PROFDEF=NO specified.

**System action:** RACF command processing ends.

**ICH10317I**  'FROM' profile profile-name is defined in database, but is not active. SETROPTS REFRESH may be required.

**Explanation:** The profile name specified in the FROM operand is not active.

**System action:** Command processing stops.

**User response:** Issue the SETROPTS REFRESH command to activate the profile.

**ICH10318I** Profile cannot be created in the class-name-1 class because profile class-name-2 has been deleted from the CDT class.

**Explanation:** You tried to define a profile in the class-name-1 class, but it was unsuccessful because that profile is related to a dynamic class that is being deleted. The class-name-2 class is present in the dynamic class descriptor table, but the class definition (the profile class-name-2 in the CDT class) has been deleted from the CDT class. When the SETROPTS RACLIST(CDT) REFRESH command is issued or the system is restarted, the class will be removed from the dynamic class descriptor table. Therefore, no profiles may be added that are in the class-name-2 class or that are related to the class-name-2 class.

For example, you tried to define a profile in the HORSES8 class, and received the following message:

**ICH10318I** Profile cannot be created in the HORSES8 class because the profile HORSES8 has been deleted from the CDT class.

This means that the system administrator is planning to remove the HORSES8 class from the class descriptor table, and as part of the removal, has already deleted the HORSES8 profile from the CDT class. Since the HORSES8 profile in the CDT class contained the definition of the HORSES8 dynamic class, profiles may no longer be added to the HORSES8 class.

As another example, you tried to define a profile named HORSES8 in the GLOBAL class (RDEFINE GLOBAL HORSES8), and received the following message:

**ICH10318I** Profile cannot be created in the GLOBAL class because the profile HORSES8 has been deleted from the CDT class.

Again, this means that the system administrator is planning to remove the HORSES8 class from the class descriptor table, and as part of the removal, has already deleted the HORSES8 profile from the CDT class. Since the HORSES8 profile in the GLOBAL class depends on the definition of the HORSES8 dynamic class, the HORSES8 profile may not be added to the GLOBAL class.

**System action:** Command processing is halted, and the profile is not added to the RACF database. If several profile names were specified on the command and class-name-1 and class-name-2 are the same, none of the profiles are added to the RACF database.

**User response:** If you intend to define the profile in the class-name-1 class, you must first define the class-name-2 class and its class attributes in the CDT class, issue the SETROPTS RACLIST(CDT) REFRESH command, and then issue the command again. For more information about adding a class to the dynamic class descriptor table, see [z/OS Security Server RACF Security Administrator’s Guide](https://www.ibm.com).
resource name does not match the expected profile name.

System action: Command completes successfully.

User response: Notify the system administrator to review and change member names, if necessary.


To delete RACFVARS members from an existing member list, use the RALTER command with the DELMEM operand. To reorder a RACFVARS member list, delete the variable by using RDELETE, and redefine it. To list a RACFVARS member list, use the RLIST command.

Note: The RLIST command lists the members of the RACFVARS in alphabetic order, not in the order entered. You can also run the IRRDBU00 data base unload utility and look at the order of the unloaded member data.

ICH10321I The profile name profile_name contains generic characters, but generics are not enabled for class class_name. A discrete profile has been created.

Explanation: You defined a discrete profile with a name containing one or more generic characters, but the class is not enabled for generic profiles. The profile profile_name only protects the single resource that matches the specified name.

System action: The discrete profile is defined. If the specified class is subsequently enabled for generic profiles, the profile profile_name becomes unusable.

User response: If you intended to create the profile as discrete, no action is necessary. If you intended to create a true generic profile, delete the discrete profile, then enable the class for generic profiles and re-issue the RDEFINE command.
RALTER command messages

**ICH11001I**  NOT AUTHORIZED TO SPECIFY
GLOBALAUDIT FOR profile-name; OPERAND IGNORED

**Explanation:** You do not have sufficient authority to specify the GLOBALAUDIT operand for the profile indicated in the message.

**System action:** RACF ignores the operand. Command processing continues with the next operand.

**User response:** See your RACF security administrator.

**ICH11002I**  AUTHORIZED TO ISSUE ONLY
GLOBALAUDIT FOR profile-name; REMAINING OPERANDS IGNORED

**Explanation:** You have specified operands in addition to GLOBALAUDIT, but you are only authorized to specify the GLOBALAUDIT operand for the indicated profile name.

**System action:** RACF ignores all operands other than GLOBALAUDIT.

**User response:** See your RACF security administrator.

**ICH11003I**  NOT AUTHORIZED TO SPECIFY
OWNER FOR profile-name; OPERAND IGNORED

**Explanation:** You do not have sufficient authority to specify the OWNER operand for the indicated profile name.

**System action:** RACF ignores the OWNER operand. Command processing continues with the next operand.

**User response:** See your RACF security administrator.

**ICH11004I**  operand DOES NOT APPLY TO
class-name CLASS ENTITIES; OPERAND IGNORED

**Explanation:** The indicated operand does not apply to the indicated class.

**System action:** RACF ignores the operand. Command processing continues with the next operand.

**ICH11005I**  LIST OF ENTITY NAMES SPECIFIED;
operand OPERAND IGNORED

**Explanation:** You have specified a list of entity names (profile names). Only a single entity name is allowed when either of the following conditions is true:
- The ADDVOL or DELVOL operand is specified.
- The class name is specified as GLOBAL or SECDATA, and the ADDMEM or DELMEM operands are specified.

**System action:** RACF ignores the operand. Command processing continues with the next operand.

**ICH11006I**  NOT AUTHORIZED TO SPECIFY
ADDVOL; OPERAND IGNORED

**Explanation:** You do not have sufficient authority to specify the ADDVOL operand.

**System action:** RACF ignores the operand. Command processing continues with the next operand.

**User response:** See your RACF security administrator.

**ICH11007I**  entity NAME CANNOT BE SPECIFIED
IN DELVOL LIST; profile-name NOT DELETED

**Explanation:** The profile name indicated by profile-name matches one of the volume serial numbers specified by the DELVOL operand.

**System action:** RACF ignores the request to delete the profile name. Command processing continues with the next volume serial number specified on the DELVOL operand.

**ICH11008I**  {seclevel-name | category-name} TO BE
DELETED SHOULD BE REMOVED
FROM ALL USER AND RESOURCE
PROFILES

**Explanation:** A category or security level has been deleted from a profile in the SECDATA class. The security categories or security levels that correspond to the name(s) deleted should be deleted from all user and resource profiles or unexpected errors in RACF processing might occur.

**ICH11009I**  RACLISTED PROFILES FOR class-name
WILL NOT REFLECT THE UPDATE(S)
UNTIL A SETROPTS REFRESH IS
ISSUED

**Explanation:** The profile class exists in common storage, but the profile updates do not become effective until the SETROPTS command is issued with the REFRESH operand. If a RALTER command was issued that did not change anything, it is not necessary to update the RACLISTED profiles through the SETROPTS REFRESH.

If this message is received for a class whose profiles contain segments other than the base segment, you should RACLST REFRESH the class immediately because only the base segments are kept in common storage, until you issue the SETROPTS RACLST REFRESH command, the copy of the base segment in storage and the segments in the database might not match, and this mismatch might cause unexpected results.
ICH1102I  profile-name  NOT DEFINED TO CLASS  
class-name
Explanation: The indicated profile name has not been 
previously defined to RACF in the indicated class.
System action: Command processing continues with 
the next profile name.

ICH1103I  NOT AUTHORIZED TO ALTER  
profile-name
Explanation: You do not have sufficient authority to 
alter the indicated profile.
System action: Command processing continues with 
the next profile name.
User response: See the owner of the profile or your 
RACF security administrator. To display the owner of 
the profile, use the RLIST command.

ICH1104I  volser  NOT IN VOLUME SET OF  
profile-name; VOLUME NOT DELETED
Explanation: The indicated volume serial number 
(volser) specified on the DELVOL operand does not 
belong to the volume set of the indicated profile.
System action: The volume serial number is not 
deleted. Command processing continues with the next 
operand.

ICH1105I  member-name  ALREADY DEFINED TO  
GROUP profile-name
Explanation: The resource name specified on the 
ADDMEM operand is already a member of the 
resource group being altered.
System action: Command processing continues with 
the next member name.

ICH1106I  volser  ALREADY DEFINED TO CLASS  
TAPEVOL
Explanation: The volume serial number (volser) 
specified on the ADDVOL operand is already defined 
to RACF in the TAPEVOL class.
System action: Command processing continues with 
the next operand.

ICH1107I  member-name  NOT DEFINED TO  
GROUP profile-name
Explanation: The resource name specified on the 
DELMEM operand is not a member of the resource 
group being altered.
System action: Command processing continues with 
the next member name.

ICH1108I  NOT AUTHORIZED TO ADD  
member-name
Explanation: The user of the RALTER command does 
not have sufficient authority to specify the indicated 
resource name on the ADDMEM operand.
System action: Command processing continues with 
the next member name.
User response: See your RACF security administrator.

ICH1111I  SINGLEDIS IGNORED. VOLUME volser  
CONTAINS MORE THAN ONE DATA SET
Explanation: The indicated volume already contains 
more than one entry in the TVTOC.
System action: RACF ignores the SINGLEDIS operand. 
Command processing continues with the next operand.

ICH1112I  TVTOC IN USE. NOTVTOC IGNORED
Explanation: A TVTOC that protects a tape data set 
already exists.
System action: RACF ignores the NOTVTOC operand. 
Command processing continues with the next operand.

ICH1113I  DELVOL volume  PROCESSING  
IGNORED. A TVTOC ENTRY EXISTS FOR A DATA SET ON THE VOLUME.
Explanation: The DELVOL operand was specified for 
a volume that has TVTOC entries for a tape data set(s) 
on the volume. The data set(s) must be deleted before 
the volume can be deleted.
System action: Command processing continues with 
the next operand.

ICH1114I  category  ALREADY DEFINED TO  
profile-name
Explanation: The security category indicated in the 
message has already been defined in this profile.
System action: RACF ignores the operand. Command 
processing continues with the next operand.

ICH1115I  category  NOT DEFINED TO  
profile-name
Explanation: The security category indicated in this 
message has not been defined to this profile.
System action: RACF ignores the operand. Command 
processing continues with the next operand.
ICH1118I  COMMAND PROCESSING TERMINATED. NO (SECLEVELS | CATEGORIES) FOUND

Explanation: RACF cannot validate the name you specified on the SECLEVEL or ADDCATEGORY operand. This happened for one of two reasons:

- There is no SECLEVEL or CATEGORY profile.
- A profile is defined, but it does not contain any members.

System action: Command processing stops.

ICH11201I  NOT AUTHORIZED TO ISSUE command-name

Explanation: One of the following conditions is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System action: Command processing stops.

User response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or the authority required to issue the indicated command, see z/OS Security Server RACF Command Language Reference.

RACF Security Administrator Response:

ICH11301I  entity-name AND REMAINING ENTITIES NOT ALTERED

Explanation: The indicated entity name (profile name) and remaining entity names in the list were not altered because of one of the following reasons:

- A RACF-manager error occurred. In this case, the message is preceded by a RACF-manager error message explaining the error.
- A system error occurred while building in-storage profiles (using RACROUTE REQUEST=LIST) for the entity names specified by the ADDMEM operand or the member class associated with the specified class is currently inactive.
- A system error occurred while checking (with REQUEST=FASTAUTH) the user's authority to the entities specified by the ADDMEM operand.

ICH11302I  VOLUME volser AND REMAINING VOLUMES NOT (ADDED | DELETED)

Explanation: The indicated volume serial number and all remaining volumes specified on the ADDVOL or DELVOL operand were not added to or deleted from a volume set because an error occurred in the RACF manager. A RACF-manager error message precedes this message and explains the error.

System action: Command processing stops after the other operands on the command have been processed.

ICH11303I  MEMBER member-name AND REMAINING MEMBERS NOT PROCESSED FOR ENTITY entity-name

Explanation: An error occurred in the RACF-manager that prevented the resource group entity name from being added to or deleted from the resource group. A RACF-manager error message precedes this message.

System action: Other operands on the command have been processed.

ICH11304I  NOT AUTHORIZED TO ADD/DELETE member-name WITH THE OPTION SPECIFIED.

Explanation: You have attempted to add a member to, or delete a member from, a profile in the VMEVENT or VMXEVENT class. However, you specified an auditing or control option that you do not have the authority to specify. The option to which you are not authorized is part of the member-name indicated in the message.

System action: Command processing continues with the next member name.

User response: See your RACF security administrator.

ICH11305I  command-name failed. You are not authorized to specify SECLABEL or NOSECLABEL.

Explanation: The command indicated in the message was issued with the SECLABEL or NOSECLABEL operand specified. However, one of the following conditions caused the command to fail:

- The user issuing the command did not have the SPECIAL attribute and SETROPTS SECLABELCONTROL is on.
- The SECLABEL or NOSECLABEL operand was specified on the RALTER command, and SETROPTS MLSTABLE is on, but SETROPTS MLQUIET is not.

System action: Command processing is terminated.

User response: See your RACF security administrator.
ICH11306I  command-name failed. You are not authorized to alter a SECLABEL profile.

Explanation: The command indicated in the message was issued for a security label profile. However, one of the following conditions caused the command to fail:
- The user issuing the command did not have the SPECIAL attribute, and SETROPTS SECLABELCONTROL is on.
- The command indicated in the message was issued by any user while SETROPTS MLSTABLE was on, but SETROPTS MLQUIET was not.

System action: Command processing stops.
User response: See your RACF security administrator.

ICH11307I  command-name failed. NOSECLABEL is not allowed under the current RACF options.

Explanation: NOSECLABEL operand was specified on the command indicated in the message, and SETROPTS MLACTIVE is on.

System action: Command processing stops.
User response: Correct the command.

ICH11308I  command-name failed. SECLABEL seclabel-name is not currently defined to RACF.

Explanation: There is no profile in class SECLABEL whose name is the security label indicated in the message.

System action: Command processing stops.
User response: Correct the command or define the security label.

ICH11309I  SECLABEL operand ignored. It does not apply to class class-name.

Explanation: The security label operand was specified on a RACF command, but security label has no meaning for the indicated class.

System action: The profile is defined, but the SECLABEL operand is ignored.

ICH11310I  command-name failed. You are not authorized to specify SECLABEL seclabel-name.

Explanation: SECLABEL seclabel-name was specified on the command indicated in the message by a user without at least READ authority to it.

System action: Command processing stops.
User response: See your RACF security administrator.

ICH11311I  NOSECLEVEL operation ignored. You cannot specify the NOSECLEVEL keyword for SECLABEL profiles.

Explanation: The user attempted to delete the security level from a SECLABEL profile. Each SECLABEL profile must have a security level.

System action: The command processor ignores the NOSECLEVEL operand. All other operands are processed.
User response: Reconsider why you issued this command. If you want to change the security level associated with a security label, issue the RALTER command with the new security level specified on the SECLEVEL keyword.

ICH11312I  You are not authorized to define this resource as delegated.

Explanation: You have specified RACF-DELEGATED in the APPLDATA of a profile in order to designate it as being delegated. However, all of the following conditions are in effect, and they are preventing you from defining a delegated profile:
- SETROPTS SECLABELCONTROL is in effect
- You do not have the system SPECIAL attribute
- The profile contains a SECLABEL


System action: Command processing stops.

ICH11313I  WARNING: RACFVARS varname has a member that is a prefix of another member. Authorization checking may not be as expected.

Explanation: When RACF compares a resource name with a profile name containing RACFVARS, it compares the resource name with each name in the RACFVARS member list on the database. The member names are arranged in the order entered by RDEF and RALT. The oldest member name (the first name in the member list) is checked first and the last member name is checked last. Each character of the resource name is compared with each character of the RACFVARS member name. The search stops at the first match of a sequence of characters in the resource name and a RACFVARS member name.

This method of checking can cause unexpected results, for example, if the member list contains names that are a subset of other members in the list. In this case, the resource name does not match the expected profile name.

System action: Command completes successfully.
User response: Notify the system administrator to review and change member names, if necessary.
RACF Security Administrator Response:

RACF Security Administrator Response: Update the member names as appropriate. See z/OS Security Server RACF Security Administrator’s Guide for more information about RACFVARS considerations.

To delete RACFVARS members from an existing member list, use the RALTER command with the DELMEM operand. To reorder a RACFVARS member list, delete the variable by using RDELETE, and redefine it. To list a RACFVARS member list, use the RLIST command.

Note: The RLIST command lists the members of the RACFVARS in alphabetic order, not in the order entered. You can also run the IRRDBU00 data base unload utility and look at the order of the unloaded member data.
RDELETE command messages

ICH12001I ALL [SECLEVELS | CATEGORIES] SHOULD BE DELETED FROM USER AND RESOURCE PROFILES

Explanation: A CATEGORY or SECLEVEL profile in the SECDATA class was deleted from the RACF data set. The profile contained a member list. All security categories or security levels should be deleted from user and resource profiles, or unexpected errors in RACF processing might occur.

ICH12002I RACLISTED PROFILES FOR class-name WILL NOT REFLECT THE DELETION(S) UNTIL A SETROPTS REFRESH IS ISSUED.

Explanation: The profile class exists in common storage. The profile cannot be deleted until the SETROPTS command is issued with the REFRESH operand.

ICH120101I profile-name NOT DEFINED TO CLASS class-name

Explanation: The indicated profile name has not been previously defined to RACF in class class-name.

System action: Command processing continues with the next profile name in the list.

ICH120101I command-name NOT AUTHORIZED TO ISSUE command-name

Explanation: One of the following conditions is true:
• RACF is inactive.
• You are not defined to RACF and cannot issue RACF commands.

System action: Command processing stops.

ICH12201I COMMAND PROCESSING TERMINATED. USER DOES NOT HAVE SUFFICIENT AUTHORITY TO ALL DATA SETS IN THE TVTOC.

Explanation: The TAPEVOL profile cannot be deleted because the TVTOC in the profile contains data set(s) that have not yet passed their security retention period and the user does not have sufficient authority to delete them.

User response: See your RACF security administrator.

ICH12301I entity-name AND REMAINING ENTITIES NOT DELETED

Explanation: The indicated entity name (profile name) and all remaining entity names in the list were not deleted from RACF because a RACF-manager error occurred. This message is preceded by a RACF-manager error message, which explains the error.

System action: Command processing stops.

ICH12301I command-name failed. There is a less specific profile profile-name with a different SECLABEL.

Explanation: The execution of the command indicated in the message can potentially change the security label of the resource because of the existence of another, less specific profile with a different security label.

System action: Command processing stops.

ICH12303I Profile not deleted. Deleting this profile would remove the only profile that provides SECLABEL protection for one or more resources.

Explanation: You cannot delete the profile specified on the command because it is the only remaining profile...
that protects one or more resources with a security label, and the SETROPTS MLACTIVE option prevents changes to SECLABEL protection.

**System action:** Command processing stops with no effect on profiles.

**User response:** Check the spelling of the command you entered. If it is correct and you intend to delete this profile, rename or delete all resources protected by the profile, then reissue the command.

---

ICH12304I All profiles in the **class-name** class must be deleted before the CDT profile **class-name** can be deleted.

**Explanation:** The class indicated in the message is a class defined in the dynamic class descriptor table. Deleting the profile causes the class to be deleted from the dynamic class descriptor table, but there is still at least one profile defined in that class.

**System action:** Profile **class-name** is not deleted from the CDT class.

**User response:** Delete every profile in the named class, and issue the command again. For more information about deleting a class from the dynamic class descriptor table, see [z/OS Security Server RACF Security Administrator’s Guide](https://www.ibm.com/support/knowledgecenter/SSS5FS_7.3.0/com.ibm.zos.v7r3.jcmd.ich.racfse administrator guide.pdf).

If SEARCH and RLIST commands do not return any profiles for the class, your database might have generic profiles defined in that class that are hidden. This can happen if a generic profile was defined in a class that is then disabled for generics with SETROPTS NOGENCMD or NOGENERIC. Issue SETROPTS GENCMD, then search and delete any profiles found. Schedule and then undo the GENCMD carefully, as it might affect other classes sharing the same POSIT values.

---

ICH12305I Profile **profile-name** in the **class-name** class must be deleted before the CDT profile **dynamic-class-name** can be deleted.

**Explanation:** You tried to delete a profile from the CDT class, but it was unsuccessful because there is still a profile in the RACF database that is related to the dynamic class you tried to delete. The class **dynamic-class-name** indicated in the message is a class defined in the dynamic class descriptor table. Deleting the profile **dynamic-class-name** from the CDT class causes the class to be deleted from the dynamic class descriptor table, but the named profile is dependent on the definition of that dynamic class. The named profile must be deleted before deleting the dynamic class.

For example, you issued the command RDELETE CDT HORSES8, and received the following message: ICH12305I Profile HORSES8 in the GLOBAL class must be deleted before the CDT profile HORSES8 can be deleted.

Since the HORSES8 profile in the GLOBAL class is related to the dynamic class named HORSES8, you must first issue RDELETE GLOBAL HORSES8 before you issue the RDELETE CDT HORSES8 command again.

**System action:** Profile **dynamic-class-name** is not deleted from the CDT class.

**User response:** Delete the **profile-name** profile from the **class-name** class, and issue the command again. For more information about deleting a class from the dynamic class descriptor table, see [z/OS Security Server RACF Security Administrator’s Guide](https://www.ibm.com/support/knowledgecenter/SSS5FS_7.3.0/com.ibm.zos.v7r3.jcmd.ich.racfse administrator guide.pdf).

---

ICH12306I A discrete profile in class **class-name** matches the name **profile-name**. Use the keyword NOGENERIC to delete it.

**Explanation:** A discrete profile, which contains generic characters and matches the specified profile name, has been created in a class that was not enabled for generic profiles. The class has then been enabled for generic profiles and therefore the profile cannot be used for resource protection.

**System action:** The discrete profile is not deleted.

**User response:** You can remove the discrete profile by re-issuing the RDELETE command while specifying the keyword NOGENERIC.
RLIST command messages

ICH13001I NOT AUTHORIZED TO ISSUE command-name

Explanation: One of the following conditions is true:
- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System action: Command processing stops.
User response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or the authority required to issue the indicated command, see z/OS Security Server RACF Command Language Reference.

ICH13002I NOT AUTHORIZED TO LIST profile-name

Explanation: You do not have sufficient authority to list the indicated profile name.

System action: Command processing continues with the next profile name in the list.
User response: See your RACF security administrator.

ICH13003I profile-name NOT FOUND

Explanation: The indicated profile name was not found in the RACF database.

ICH13004I NOTHING TO LIST

Explanation: You specified * for profile name. Either there are no profiles in that class or you do not have sufficient authority to list any of them.

ICH13005I RESGROUP DOES NOT APPLY TO class-name CLASS ENTITIES; OPERAND IGNORED

Explanation: The RESGROUP operand was specified on the RLIST command and the specified class is not a “member class” (such as TERMINAL or DASDVOL) for which a resource grouping class exists.

System action: RACF ignores the operand. Command processing continues with the next operand.

ICH13006I No profile(s) listed. NORACF specified and no other information requested.

Explanation: NORACF was specified on the RLIST command, but no segments were requested.

ICH13007I One or more requested profiles for class-name class are defined in the database, but are not listed. RACLST REFRESH is required.

Explanation: The RLIST command lists database profiles. This message indicates that circumstances exist that prevent RACF from verifying your authority to list one or more requested profiles. This can occur when profiles in a RACLSTed class are added without doing RACLST REFRESH.

System action: Any requested profiles for the class-name class that the user is authorized to list are listed.
SETROPTS command messages

ICH14001I NOT AUTHORIZED TO ISSUE SETROPTS

Explanation: One of the following conditions is true:
- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System action: Command processing stops.

User response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or the authority required to issue the indicated command, see z/OS Security Server RACF Command Language Reference.

ICH14002I NOT AUTHORIZED TO SPECIFY keyword [keyword...]; KEYWORD IGNORED.

Explanation: You do not have sufficient authority to specify the keywords indicated.

System action: RACF ignores these keywords and continues command processing with the remaining keywords.

User response: See your RACF security administrator.

ICH14003I I/O ERROR - jji, sss, ddd, devtyp, ddn, oper, xxxx, acc

Explanation: A permanent I/O error occurred while processing on device ddd. In the message text, the error analysis information provided by the SYNADAF data management macro instruction issued by the SYNAD routine was:

- jji    Job name
- sss    Step name
- ddd    Unit address of the device
- devtyp Device type
- ddn    Data definition name
- oper   Operation attempted
- xxxx   Last seek address or block count
- acc    Access method

System action: Command processing stops.

Problem Determination: Other messages might have been issued for this problem. These messages might display on the system console or the security console, or users might receive them. An analysis of those messages might help you determine the cause of the problem. In particular, look for message ICH51011I, which reports a return code from the RACF manager.

ICH14004I UNABLE TO OPEN RACF DATA SET dsname

Explanation: The OPEN for the indicated data set failed.

System action: Command processing stops.

User response: Notify your system programmer.

System programmer response: To recover from the problem, consider switching to a backup RACF database (using the RVARY SWITCH command).

Note: For complete information about recovering from the problem, see the section on RACF database recovery in z/OS Security Server RACF System Programmer’s Guide. Pay particular attention to the section on failures during I/O operations on the RACF database in z/OS Security Server RACF System Programmer’s Guide.

Problem Determination: Other messages might have been issued for this problem. These messages might display on the system console or the security console, or users might receive them. An analysis of those messages might help you determine the cause of the problem. In particular, look for message ICH51011I, which reports a return code from the RACF manager.

ICH14006I NOT AUTHORIZED TO CHANGE RACF OPTIONS; RACF CURRENTLY INACTIVE.

Explanation: RACF has previously been set not active by the RVARY command. RACF options cannot be changed by the SETROPTS command until the RVARY command is issued and RACF is set active again.

System action: Command processing stops.
ICH14009I  RULEn HAS AN OVERLAPPING SPECIFICATION IN THE CONTENT RULES.

Explanation: You have tried to use the SETROPTS command to define a syntax rule for use in your installation. The position values for the content keywords overlap. The following example illustrates overlapping position values:

```
SETROPTS PASSWORD (RULE1(LENGTH(8) - ALPHA(1:5) NUMERIC(4:8)))
```

The overlap occurs for positions 4 and 5 in the content keywords ALPHA and NUMERIC. There are several ways to correct the error, depending on your intention for the rule. For example, ...ALPHA(1:3) NUMERIC(4:8)... is correct.

System action: RACF ignores this rule and other rules specified by RULEn but processes other PASSWORD options and other keywords specified on the SETROPTS command.

ICH14010I  * WARNING, THIS OPTION IS INACTIVE, IT REQUIRES THE ‘INITSTATS’ OPTION.

Explanation: RACF requires that the INITSTATS option is in effect when you specify the LIST operand on the SETROPTS command with any of the following options: INACTIVE, REVOKE, HISTORY, or WARNING.

System action: Command processing stops.

ICH14011I  GLOBAL ACCESS CHECKING BASE TABLE IS ABSENT, NO GLOBAL ACCESS CHECKING CAN BE DONE.

Explanation: During RACF Master Scheduler Initialization processing, an error prevented construction of the global access checking base table.

System action: Global access checking is disabled, but the GLOBAL options are set in the RACF CVT and in the RACF database ICB.

ICH14013I  REFRESH IGNORED. NO RELATED KEYWORDS SPECIFIED.

Explanation: When the REFRESH operand is specified, the GLOBAL, GENERIC, GENLIST, RACLIST, or WHEN operand must also be specified to indicate what is to be refreshed.

System action: RACF continues command processing with the other operands specified.

ICH14014I  GLOBAL ACCESS CHECKING BASE TABLE IS ABSENT, REFRESH CANNOT BE DONE.

Explanation: During RACF initialization processing, an error prevented construction of the global access checking base table. You cannot perform a global access checking refresh or generic profile checking refresh.

System action: Command processing continues with the other operands. If the system is enabled for sysplex communication, the command is propagated to other systems in the sysplex. If this condition is detected on another member of the sysplex, this message is issued on that other member’s master console as a WTO.

ICH14015I  NOT AUTHORIZED TO REFRESH [GLOBAL | GENERIC | RACLIST] CLASS class-name

Explanation: You do not have sufficient authority to refresh the given class.

System action: RACF ignores this class. Command processing continues with the next operand.

User response: See your RACF security administrator.

ICH14016I  CANNOT REFRESH class-name, [GLOBAL | GENERIC] ACCESS CHECKING INACTIVE

Explanation: Because global access checking or generic access checking is inactive for the given class, no refresh can be done.

System action: RACF ignores this class. Command processing continues with the next operand.

ICH14018I  WARNING: TAPEDSN OPTION ACTIVE, TAPEVOL CLASS IS NOT ACTIVE

Explanation: To protect tape data sets, if your installation does not have a tape management system, RACF requires the TAPEVOL class to be active.

User response: Use the SETROPTS command with CLASSACT(TAPEVOL) specified to activate the TAPEVOL class.
ICH14019I  'RVARYPW' IGNORED. ERROR ENCOUNTERED DURING PASSWORD ENCODING.

Explanation: RACF uses an installation-defined password to approve a user's issuance of the RVARY command. The password is specified in the RVARYPW operand of the SETROPTS command. If RACF is unable to encode the password at the time the SETROPTS command is issued, you receive this message.

System action: RACF ignores the operand and processing continues with the next operand.

User response: Report this message to your system programmer.

ICH14020I  'WHEN/NOWHEN' OPTION IGNORED. ENVIRONMENT DOES NOT SUPPORT class-name CLASS

Explanation: Because it does not support the indicated class, RACF cannot implement the WHEN or NOWHEN option in this system environment.

System action: RACF ignores the option.

ICH14021I  ERROR REFRESHING program ACCESS TABLE. COMMAND PROCESSING TERMINATED

Explanation: An error occurred when RACF attempted to refresh the program access table.

System action: Command processing stops.

ICH14023I  ERROR ENCOUNTERED DURING RAclist, NORaclist, OR RACLlist REFRESH PROCESSING. SYSTEM STORAGE MAY NOT HAVE BEEN RECOVERED.

Explanation: An error occurred during RAclist, NORaclist, or RACLlist REFRESH processing, which might have caused storage loss.

ICH14024I  SECDATA SECLEVEL PROFILE NOT FOUND ON RACF DATASET. COMMAND PROCESSING TERMINATED.

Explanation: No profile named SECLEVEL is defined in class SECDATA.

ICH14025I  ERROR ENCOUNTERED DURING SECLEVEL PROCESSING. COMMAND PROCESSING TERMINATED.

Explanation: An error occurred when RACF attempted to process the SECLEVEL operand.

System action: Command processing stops.

ICH14026I  NOT PROCESSED FOR class-name, RAclist AND GENLIST CANNOT BOTH BE ACTIVE.

Explanation: You cannot specify both RAclist and GENLIST for the same general resource class.

User response: Reissue the command, specifying either RAclist or GENLIST.

ICH14027I  (RAclist | GENLIST) OF CLASS class-name NOT ALLOWED BY THE CLASS DESCRIPTOR TABLE. OPERAND IGNORED.

Explanation: The definition in the class descriptor table does not allow this class to be RAclistEd or GENLISTed.

System action: RACF ignores the option.

ICH14028I  CLASS class-name ALREADY GENLISTED. OPERAND IGNORED.

Explanation: A class can be GENLISTed only once. The class specified has already been GENLISTed by using the SETROPTS command and cannot be GENLISTed again.

System action: RACF ignores the option.

ICH14030I  NOGENLIST of class class-name ignored. GENLIST has not been done yet.

Explanation: SETROPTS NOGENLIST is valid only for classes for which SETROPTS GENLIST has been successful.

System action: None of the classes specified on the NOGENLIST operand was affected.

User response: If you do not want profiles kept in storage for this class, do nothing. If you have specified more than one class on the NOGENLIST operand, none of the classes is affected by the command. Issue the SETROPTS command again, omitting the class indicated in the message from the NOGENLIST operand.

ICH14031I  request of class class-name failed.

Explanation: The SETROPTS command was issued with one of the following specified:

- RAclist
- RAclist REFRESH
- NORaclist
- NOGENLIST
- NOGENERIC

The request did not complete successfully.

Note: This message is displayed in uppercase when issued to the operator console.
ICH14032I  No in-storage profiles were found for class class-name.

Explanation: The SETROPTS command was issued with one of the following specified:
- NOGENLIST
- NOGENERIC

The request did not complete successfully.

System action: The class indicated in the message was not affected by the SETROPTS command.

User response: Check that the class-name specified in the SETROPTS command is the class you want. If it is, the class does not have the necessary profiles.

ICH14033I  Return code from RACLIST macro is return-code.

Explanation: The SETROPTS command processor encountered an error related to the RACROUTE REQUEST=LIST macro.

Note: This message is displayed in uppercase when issued to the operator console.

System action: The class indicated in message ICH14031I was not affected by the SETROPTS command. If the system is enabled for sysplex communication and the error occurred on the coordinating system, the command is not propagated or processed. If the error occurred on a peer system and the coordinating system is running in data sharing mode, the command stops processing on all systems. Otherwise, processing continues.

User response: If the message indicates a return code other than zero, issue the SETROPTS command again. If the problem persists, see your system programmer.

System programmer response: See “Problem Determination.”

Problem Determination: If the return code reported in this message is not zero, see the description of return codes for the REQUEST=LIST macro in the z/OS Security Server RACROUTE Macro Reference.

ICH14034I  Reason code from RACLST LIST macro is reason-code.

Explanation: The SETROPTS command processor issued the RACROUTE REQUEST=LIST macro, but received the return code reported in message ICH14033I. This message reports a related reason code.

ICH14035I  RACINIT {CREATE | DELETE} failed, return code return-code.

Explanation: If the message indicates CREATE, then SETROPTS RACLIST processing cannot create an ACEE. If the message indicates DELETE, then SETROPTS RACLIST processing cannot delete an ACEE.

Note: This message is displayed in uppercase when issued to the operator console.

System action: If the system is not enabled for sysplex communication, command processing stops and no classes are affected. If the system is enabled for sysplex communication, command processing stops and no classes are affected. If the system is enabled for sysplex communication and the error occurred on the coordinating system, the command is not propagated or processed. If the error occurred on a peer system and the coordinating system is running in data sharing mode, the command stops processing on all systems. Otherwise, processing continues.

User response: Issue the SETROPTS command again. If the problem persists, report the exact text of this message to your system programmer.

System programmer response: To correct the problem, re-IPL the system. If the problem persists, see “Problem Determination.”

Problem Determination: For a description of the
ICH14036I Unable to [ENQ | DEQ] the class descriptor table.

Explanation: If ENQ is specified in the message, SETROPTS RACLIST (or GENLIST) processing cannot obtain an exclusive lock on the class descriptor table. If DEQ is specified in the message, SETROPTS RACLIST (or GENLIST) processing cannot release its lock on the class descriptor table.

System action: Command processing stops and no classes are affected.

User response: Issue the SETROPTS command again. If the problem persists, see your system programmer.

System programmer response: To correct the problem, re-IPL the system. If the problem persists, see “Problem Determination.”

Problem Determination: Report the exact text of this message, with the exact wording of the SETROPTS command you entered, to your IBM support center.

ICH14037I WARNING! The MLS option is active, but the SECLABEL class is inactive.

Explanation: The SETROPTS MLS command was issued, but the SECLABEL class is not active.

System action: There is no effect on system operation.

User response: To put the MLS option into effect, activate the SECLABEL class.

ICH14038I WARNING! The MLACTIVE option is active, but the SECLABEL class is inactive.

Explanation: The SETROPTS MLACTIVE command was issued, but the SECLABEL class is not active.

System action: There is no effect on system operation.

User response: To put the MLACTIVE option into effect, activate the SECLABEL class.

ICH14040I WARNING! You must RACLIST class class-name before authorization checking can occur.

Explanation: This message is issued when a class is activated by way of the SETROPTS CLASSACT(class) command, and the RACF class descriptor table indicates that this class must be RACLISTed before checking can occur.

System action: RACF does not perform authorization checking (or auditing based on profiles) for the class until the indicated class has been RACLISTed.

User response: Issue the SETROPTS RACLIST command for the class.

ICH14041I action of class class-name ignored. The class is not active yet.

Explanation: The SETROPTS command was issued with the RACLIST or RACLIST REFRESH operands specified. However, class class-name is not active.

System action: SETROPTS RACLIST processing is not done for the class.

User response: Activate the class and issue the SETROPTS RACLIST command.

ICH14042I action of class class-name ignored. The class has been marked for de-activation.

Explanation: The SETROPTS command was issued with the NOCLASSACT and RACLIST operands specified and did not complete successfully.

System action: Class class-name was not affected by the SETROPTS command.

User response: You cannot specify both the NOCLASSACT operand and the RACLIST operand for the same class. Correct the command and try again.

ICH14043I Invalid character character specified in the userid for operand. Operand ignored.

Explanation: The user ID specified on the JES(NJEUSERID) or JES(UNDEFINEDUSER) operand contained an incorrect character.

System action: RACF ignores operand operand.

User response: Change the user ID specified in the command and try again.

ICH14044I Userid userid specified for operand already exists. Please try another userid.

Explanation: The user ID specified on the JES(NJEUSERID) or JES(UNDEFINEDUSER) operand is already a RACF-defined user.

System action: RACF ignores operand operand.

User response: Change the user ID specified in the command and try again.

ICH14045I RACXTRT macro for operand failed.

Explanation: While processing the SETROPTS command, RACF issued the RACROUTE REQUEST=EXTRACT macro, and an error occurred.

System action: Command processing stops.

User response: Report the exact text of this message,
ICH14046I  Return code is return-code, reason code is reason-code.

Explanation: This message follows message ICH14045I, and includes additional problem determination information for the error that caused message ICH14045I.

System action: See message ICH14045I.

User response: See message ICH14045I.

ICH14047I  Return code from RACROUTE macro is return-code.

Explanation: This message follows message ICH14045I, and includes additional problem determination information for the error that caused message ICH14045I. Various RACF macros are invoked by RACROUTE. If either the RACROUTE interface or the called macro fails, the RACROUTE macro returns its own return code and the return and reason codes of the called macro. For example, if the RACROUTE return code is 4, and the RACROUTE REQUEST=LIST return and reason codes are 0, this means that the class is not in the router table and the REQUEST=LIST processing was not done.

Note: This message is displayed in uppercase when issued to the operator console.

System action: See message ICH14045I.

User response: See message ICH14045I.

ICH14048I  Security level name security-level-name is not defined to RACF.

Explanation: An incorrect security level name was entered on a SETROPTS ERASE-ON-SCRATCH BY SECLEVEL or SETROPTS SECLEVELAUDIT option.

System action: The system prompts the user to reenter the command.

User response: Check the spelling of the value specified for the security-level name and reenter the command.

ICH14049I  The PRIMARY sub-operand was ignored. value is not a valid language code.

Explanation: The specified PRIMARY sub-operand value is not one of the 3-letter codes defined by IBM.

System action: The installation default for the PRIMARY language is not changed. Processing continues with the next operand or sub-operand.

User response: Issue the SETROPTS command again with a valid language code specified.

ICH14050I  The PRIMARY sub-operand was ignored. The MVS message service is not active.

Explanation: The specified PRIMARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was assumed to be an installation-defined language name, but the required language code cannot be obtained because the MVS message service is not active.

System action: The installation default for the PRIMARY language is not changed. Processing continues with the next operand or sub-operand.

User response: Issue the SETROPTS command again with a valid language code specified.

ICH14051I  The SECONDARY sub-operand was ignored. value is not a valid language code.

Explanation: The specified SECONDARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was assumed to be an installation-defined language name, but the required language code cannot be obtained from the MVS message service.

System action: The installation default for the SECONDARY language is not changed. Processing continues with the next operand or sub-operand.

User response: Issue the SETROPTS command again with a valid language code or language name specified.

ICH14052I  The SECONDARY sub-operand was ignored. value is not a valid language code.

Explanation: The specified SECONDARY sub-operand value is not one of the 3-letter codes defined by IBM.

System action: The installation default for the SECONDARY language is not changed. Processing continues with the next operand or sub-operand.

User response: Issue the SETROPTS command again with a valid language code specified.
ICH14053I The SECONDARY sub-operand was ignored. The MVS message service is not active.

Explanation: The specified SECONDARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was assumed to be an installation-defined language name, but the required language code cannot be obtained because the MVS message service is not active.

System action: The installation default for the SECONDARY language is not changed. Processing continues with the next operand or sub-operand.

User response: Issue the SETROPTS command again with a valid language code specified.

ICH14054I The SECONDARY sub-operand was ignored. The specified language is not active.

Explanation: The specified SECONDARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was assumed to be an installation-defined language name, but the required language code cannot be obtained from the MVS message service.

System action: The installation default for the SECONDARY language is not changed. Processing continues with the next operand or sub-operand.

User response: Issue the SETROPTS command again with a valid language code or language name specified.

ICH14055I The PRIMARY sub-operand was ignored. QRYLANG failed with return code xxxx and reason code yyy.

Explanation: The specified PRIMARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was assumed to be an installation-defined language name, but the required language code cannot be obtained because an error condition occurred when the QRYLANG macro of the MVS message service was executing. The return code is indicated by xxxx. The reason code is indicated by yyy.

System action: The system-wide default for the PRIMARY language is not changed. Processing continues with the next operand or sub-operand.

User response: Report the complete text of this message to your system programmer.


ICH14056I The SECONDARY sub-operand was ignored. QRYLANG failed with return code xxxx and reason code yyy.

Explanation: The specified SECONDARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was assumed to be an installation-defined language name, but the required language code cannot be obtained because an error condition occurred when the QRYLANG macro of the MVS message service was executing. The return code is indicated by xxxx. The reason code is indicated by yyy.

System action: The system-wide default for the SECONDARY language is not changed. Processing continues with the next operand or sub-operand.

User response: Issue the SETROPTS command again with a valid language code or language name specified.


ICH14058I request of class classname encountered a data space problem. Return code is return-code, reason code is reason-code.

Explanation: The SETROPTS command processor encountered a problem creating a data space, deleting a data space, or moving data into a data space. The request can be one of the following:

- RACLST
- RACLST REFRESH
- NORACLST

Note: This message is displayed in uppercase when issued to the operator console.

System action: If this message is preceded by message ICH14031I, data space processing is the reason the command failed. If not, the command completed in spite of the data space problems. The return and reason codes can help the IBM support center determine the cause of the problem. In addition to issuing this message, the system might also have taken an SVC dump.

If the system is enabled for sysplex communication and the error occurred on the coordinating system, the command is not propagated or processed. If the error occurred on a peer system and the coordinating system is running in data sharing mode, command processing stops on all systems. Otherwise, processing continues.

There is an exception in sysplex processing for the CDT class; if the dataspace error occurs during RACLST processing of the CDT class on any system, the command is ignored on that system and processing continues on the other systems.

User response: If the SETROPTS command failed,
ICH14059I • ICH14061I

re-issue it. If the problem recurs, report the exact text of this message to your system programmer.

System programmer response: Perform problem determination.

Problem Determination: Report the issuance of this message plus the exact wording of the SETROPTS command you entered to your IBM support center. Have the return and reason codes, and the SVC dump if one was taken, available.

<table>
<thead>
<tr>
<th>Return Code</th>
<th>Reason Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>04</td>
<td>04</td>
<td>ALESERV ADD function failed</td>
</tr>
<tr>
<td>08</td>
<td>04</td>
<td>TCBTOKEN function failed</td>
</tr>
<tr>
<td>08</td>
<td>08</td>
<td>DSPSERV CREATE function failed</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>ALESERV ADD function failed</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td>DSPSERV Delete failed</td>
</tr>
</tbody>
</table>

Note: These return codes and reason codes are described in **z/OS MVS Programming: Authorized Assembler Services Guide**.

ICH14059I  Class class-name was not activated by the SETROPTS CLASSACT(*) command.

Explanation: The SETROPTS CLASSACT(*) command was issued and the class indicated in the message has a default return code of 8 in the class descriptor table. This class should be activated explicitly.

System action: The class indicated in the message was not affected by the SETROPTS command.

User response: If you want this class to be activated, ensure that profiles have been defined for this class, then use SETROPTS class-name to activate it.

ICH14064I  ALESERV ADD function failed with return code X’reetcode’ during SETROPTS raclist-type command processing for class classname.

Explanation: The system is enabled for sysplex communication and a SETROPTS RACLIST or SETROPTS RACLIST REFRESH command encountered an ALESERV ADD error while trying to obtain an ALET during the creation of a new data space. This message occurs only on the peer system.
ICH14065I  Class *classname* not defined in class descriptor table (CDT).

Explanation: The system is enabled for sysplex communication and a coordinated SETROPTS command was issued on another system in the sysplex to perform some type of operation on the specified class. That class is not defined in the class descriptor table on this system.

Note: This message is displayed in uppercase when issued to the operator console.

System action: The command is ignored on this system but is processed on other systems where *classname* is defined in the class descriptor table.

User response: Check with your system programmer to determine if the class should be added to the class descriptor table.

ICH14066I  Error refreshing global access table for class *classname*.

Explanation: The system is enabled for sysplex communication and an error occurred when RACF attempted to update the global access table on this system.

Note: This message is displayed in uppercase when issued to the operator console.

System action: If the error occurred on the coordinating system, the command is not propagated or processed. If the error occurred on a peer system and the coordinating system is running in data sharing mode, the command stops processing on all systems. Otherwise, processing continues on systems where the command can be processed successfully.

ICH14067I  Coordinated SETROPTS operation failed on one or more members of the RACF group. Command processing continues.

Explanation: The system is enabled for sysplex communication and a SETROPTS command was propagated to other members in the sysplex. One or more of these members failed to execute the command, but command processing continues.

User response: Check the system log for message IRRX0061 to identify the members that experienced the failure. Consult the system logs for each failing member for messages or additional information.

ICH14068I  Coordinated SETROPTS operation failed on one or more members of the RACF group. Command processing stops.

Explanation: The system is enabled for sysplex communication and a SETROPTS command was propagated to other members in the sysplex. One or more of these members failed to execute the command, and command processing stopped for the class named in the message sent to the peer member, and continues for the other classes, if any, in the scope of the SETROPTS command.

User response: Check the system log for message IRRX0061 to identify the peer members that experienced the failure. Consult the system logs for each failing peer member for messages or additional information.

ICH14069I  Error refreshing program access table.

Explanation: The system is enabled for sysplex communication and an error occurred when RACF attempted to refresh the program access table on this system.

Note: This message is displayed in uppercase when issued to the operator console.

System action: If the error occurred on the coordinating system, the command is not propagated or processed. If the error occurred on a peer system and the coordinating system is running in data sharing mode, the command stops processing on all systems. Otherwise, processing continues on systems where the command can be processed successfully.

ICH14070I  SETROPTS raclist-type had no effect on class *classname*.

Explanation: One of the following conditions occurred:
- A SETROPTS RACLST was issued and this class was already SETROPTS RACLSTed.
ICH14071I  SETROPTS raclist-type had no effect on
class classname except to alter
RACGLIST profiles.

Explanation: One of the following conditions occurred:

- A SETROPTS RAclist REFRESH or SETROPTS NORACLIST command was issued and this class was not RAclistEd by either a SETROPTS RAclist command or a RACROUTE REQUEST=LIST,GLOBAL=YES request. A SETROPTS RAclist command was issued and this class was not RAclistEd by either a SETROPTS RAclist command or a RACROUTE REQUEST=LIST,GLOBAL=YES request.

In either case, if this system is enabled for sysplex communication, this message applies to all members of the sysplex.

System action: The command had no effect on this class.

User response: Check that the classname specified on the original command is the class you want. SETROPTS raclist-type commands process all the classes with the same posit as the class specified in the command. Therefore, classname in this message might not be the class specified in the command. Issue a SETROPTS LIST command to verify classes that are RAclistEd.

ICH14073I WARNING: Class class-name was
activated by the SETROPTS command.
Authorization checks might fail.

Explanation: As a result of a SETROPTS CLASSACT command, class class-name was activated. This class has a default return code of 8 in the class descriptor table and has no profiles. All authorization checks for resources in this class will fail unless overridden by an installation exit.

System action: The class, class-name, was activated. Other classes with the same POSIT value, if any exist, were also activated. No message is issued for those classes.

User response: If you want class class-name to remain active, be sure that profiles are not required for this class or that the appropriate installation exits are installed (for example, ICHRXC01 or ICHRXC02).

Because authorization checks to any resource in the class fail without appropriate exits, you might want to deactivate the class by issuing the SETROPTS NoclASSACT(class-name) command.

System programmer response: See Server RACF Macros and Interfaces for an explanation of shared POSIT values, for instructions on how to change the POSIT value for a class, or for an explanation of default return code 8.

ICH14074I WARNING: Generic profiles created
with EGN in effect might not protect
resources when NOEGN is in effect.

Explanation: EGN (enhanced generic naming) was in effect and NOEGN was specified on the SETROPTS command. Some generic profiles containing an * or ** that were created while EGN was in effect, will not protect any resources when NOEGN is in effect. For example, profile ‘USER1.AB.**.CD’ protects USER1’s data sets AB.CD and AB.EF.CD when EGN is in effect. ‘USER2.GH.*’ protects USER2’s data sets GH.IJ and GH.KL. The profiles, created when EGN was in effect, are not recognized when NOEGN is in effect and do not protect any resources.
**System action:** The command proceeds and NOEGN is placed in effect.

**User response:** Do one of the following tasks:

- If the change to NOEGN caused some resources to become unprotected, issue SETROPTS EGN to place EGN in effect.
- If placing NOEGN in effect does not leave resources unprotected, then no action is required.

Contact your system administrator if you need help determining if any resources must be protected.

**RACF Security Administrator Response:** Be sure that no resources are left unprotected when NOEGN is placed in effect. Use the SEARCH and LISTDSD commands to determine what profiles are defined and which profile protects a particular resource. See "Naming Considerations For Resource Profiles" in z/OS Security Server RACF Command Language Reference for a discussion of the differences between generic profile protection with EGN and NOEGN.

**ICH14075I** SETROPTS keyword had no effect on class classname.

**Explanation:** SETROPTS keyword was issued for the class classname. However, this class does not support generic profile checking, or generic profile command processing, so the keyword option cannot be activated for this class.

**System action:** RACF ignores this class. Command processing continues with the next operand.

**ICH14076I** The option-name option cannot be activated because the SECLABEL class is inactive.

**Explanation:** The SETROPTS command was issued in attempting to activate the MLFSOBJ, MLIPCOBJ or SECLBSYS option, but the SECLABEL class is not active.

**System action:** The option specified by option-name was not activated.

**User response:** Reissue the command after activating the SECLABEL class.

**ICH14077I** Active multi-level security options do not allow the deactivation of the SECLABEL class.

**Explanation:** The SETROPTS command was issued in attempting to deactivate the SECLABEL class, but at least one of the options requiring it is active.

**System action:** The SECLABEL class was not deactivated by the SETROPTS command.

**User response:** Deactivate the options and try again.

**ICH14078I** Unable to signal RACLIST change. ENFREQ failed with return code xxx.

**Explanation:** SETROPTS command processing attempted to use the Event Notification Facility to signal a RACLIST change for a class with SIGNAL=YES specified in its class descriptor table entry. The ENFREQ macro failed with the return code indicated by xxx.

**Note:** When RACF is enabled for sysplex communications, the SETROPTS RACLIST, RACLIST REFRESH, or NORAelist option can be propagated. This message might display on the coordinator system from where the SETROPTS was issued similar to a typical SETROPTS message, or might appear on the peer system. If on the peer system, the descriptor code is 4 and the routing code is 2.

**System action:** SETROPTS processing completes successfully, but other components might not react properly to the change in RACLISTed profiles.

**User response:** Report the complete text of this message to your system programmer.

**System programmer response:** See z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG for a description of return codes for the ENFREQ macro. Report the problem to the IBM Support Center.

RACROUTE REQUEST=FASTAUTH can issue the following diagnostic messages when performing conditional access list checking for the SERVAUTH class (specifically Program Access to SERVAUTH). The ICH prefix is used for consistency with the ICH408I authorization failure message that often follows the new messages. The new messages are issued when LOG=ASIS is specified on RACROUTE REQUEST=FASTAUTH, and MSGSUPP=YES is not specified. They are not returned by MSGRTRN=YES.

**Note:** Messages ICH420I and ICH421I might also be issued by FASTAUTH processing for SERVAUTH profiles with conditional access lists. These are saved messages that indicate why the environment became uncontrolled, causing the conditional access list checking to be bypassed.

**ICH14079I** RACF detected an error in the dynamic class descriptor table, entry entry-name, error code yy.

**Explanation:** RACF encountered an error for entry entry-name while building the dynamic class descriptor table. The entries used to build this table are taken from the class definitions in the CDT general resource class. Error code yy identifies the problem as follows:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description of error</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Incorrect class name.</td>
</tr>
</tbody>
</table>
ICH14080I

2 The field that defines the length of the class name (MAXLENGTH or MAXLENX) is incorrect. The valid range is 1 to 246.

3 The MAXLENX value must be greater than or equal to the MAXLENGTH value.

4 The maximum number of classes in the static class descriptor table (ICHRRCDX and ICHRRCDE) and the dynamic class descriptor table has been exceeded. The maximum number of classes allowed is 1024.

5 Incorrect or missing POSIT number. The valid range is 0 to 1023.

6 One of the following conditions:
   - A grouped class specifies a member that does not exist in the class descriptor table or is incorrect, or a member class specifies a group that does not exist in the class descriptor table or is incorrect.
   - A pair of classes reference each other, but neither is a grouping class or both are grouping classes.

7 One of the reserved class names (USER, GROUP, or DATASET) appears in the class table.

8 An entry in the dynamic class descriptor table has a class name with the same name as an entry in the table supplied by IBM.

9 The class specifies both MEMBER and GROUP, but they are mutually exclusive.

10 Incorrect DEFAULTRC value. The valid values are 0, 4, and 8.

11 Incorrect KEYQUALIFIERS value. The valid range is 0 to 123.

12 SIGNAL(YES) is not valid with GENLIST(ALLOWED).

13 CDTINFO segment is missing.

14 A class of the same name is also in the installation-defined class descriptor table (ICHRRCDX) and one of the following conditions is true:
   - The member class name in the dynamic class is different from the member class name in the installation-defined class.
   - The grouping class name in the dynamic class is different from the grouping class name in the installation-defined class.
   - The dynamic class is a grouping class and the installation-defined class is not a grouping class.
   - The dynamic class is a member class and the installation-defined class is not a member class.

15 GENERIC(DISALLOWED) is not valid with GENLIST(ALLOWED).

16 There are too many profiles in the CDT class for the SETROPTS command to process. Any remaining entries are not processed.

Note: This message is displayed in uppercase when issued to the operator console.

System action: The named entry is not placed in the dynamic class descriptor table, so the class is not available for RACF processing.

User response: Examine the profile entry-name in the CDT general resource class. If it was created incorrectly with a wrong name, delete the profile and create it with the correct name. The name cannot be USER, GROUP, DATASET, or any class in the IBM-supplied class descriptor table. For the list of classes in the IBM-supplied table, see z/OS Security Server RACF Macros and Interfaces. If the profile was created with an incorrect value in a CDTINFO field (such as MEMBER, GROUP, MAXLENGTH), use the RALTER command to correct the field and rebuild the dynamic class descriptor table. If the profile was created with no CDTINFO segment, use the RALTER command to add the CDTINFO segment with appropriate information, and then rebuild the dynamic class descriptor table.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

ICH14080I  Warning: RACF detected a possible error in the dynamic class descriptor table, entry entry-name, error code yy. The class is available for further processing.

Explanation: RACF encountered a possible error for entry entry-name while building the dynamic class descriptor table. The entries used to build this table are taken from the class definitions in the CDT general resource class. Error code yy identifies the problem as follows:

Code Description of error
1 The class name does not contain a national character nor a number. To ensure IBM does not create an IBM-defined class in the future by this same name, you should choose a class name that contains at least one national character or a number.

2 The POSIT value is not within the recommended ranges for a class in the dynamic class descriptor table (19-56, 128-527). This is acceptable only if your class is sharing a POSIT value with an IBM-defined class. If you chose a POSIT value that is not currently used for an IBM-defined class, be aware that IBM might in the future create an IBM-defined
class with this POSIT number; if this happens at a later date, results for your class are unpredictable.

Note:
- This message is displayed in uppercase when issued to the operator console.
- This message is not issued on releases after z/OS V1R6.0.

System action: The named entry is placed in the dynamic class descriptor table and is available for further processing on RACF commands and macros.

User response: Examine the profile class-name in the CDT general resource class. If it was created incorrectly with a wrong name, delete the profile and create it with the correct name. If the profile was created with an incorrect value in a CDTINFO field (such as MEMBER, GROUP, MAXLENGTH), use the RALTER command to correct the field and rebuild the dynamic class descriptor table.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

ICH14081I Warning: Class class-name is in the dynamic class descriptor table and also in the installation-defined class descriptor table (ICHRRCDE). The definition in the dynamic class descriptor table is now in use for RACF processing.

Explanation: RACF encountered a duplicate class name in the dynamic class descriptor table and the installation-defined class descriptor table (module ICHRRCDE). The class attributes in the dynamic class table override any class attributes in ICHRRCDE.

Note: This message is displayed in uppercase when issued to the operator console.

System action: The class definition in ICHRRCDE is used for further RACF processing, since the definition in the dynamic class descriptor table is no longer active or was removed.

User response: The duplication of class names in the dynamic class descriptor table and the installation-defined class descriptor table is allowed for a migration period. No further action is required if you intentionally deactivated the dynamic class descriptor table or removed the class from the dynamic class descriptor table.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

ICH14083I Minimum change interval exceeds the password interval.

Explanation: The value specified for MINCHANGE exceeds the installation-specified maximum set by SETR PASSWORD(INTERVAL).

System action: RACF ignores the operand and continues command processing with the next operand.

RACF Security Administrator Response: Issue SETR LIST to check the current minimum and maximum values and specify correct values.

ICH14084I ICHEINTY LOCATE failure on profile-name in class LDAPBIND, return code = X'xxxxxxxx' and reason code = X'yyyyyyyy'.

Explanation: An unexpected return code was received from ICHEINTY while attempting to retrieve information from the specified profile-name in the LDAPBIND class. The ICHEINTY return code as specified by xxxxxxxx, and the reason code as specified by yyyyyyyyy are given in hexadecimal.

Note: When RACF is enabled for sysplex communications, the SETROPTS RACLIST or RACLIST REFRESH is propagated. This message
ICH14085I

might display on the coordinator system from which the SETROPTS was issued like a typical SETROPTS message, or it might appear on the peer system. If on the peer, the descriptor code is 4. The routing code is 2.

**System action:** SETROPTS RAclist or RAclist REFRESH processing continues. The identity cache configuration is **not** changed.

**Operator response:** Report the exact text of this message to your system programmer.

**System programmer response:** See z/OS Security Server RACF Macros and Interfaces for the description of the return and reason codes for the ICHEINTY macro. Determine the cause of the error, correct it, and try again. If the problem persists, contact your RACF Security Administrator.

---

ICH14085I

*Warning:* `keyword-1` was changed to `keyword-2` for class `class-1` because the class shares a POSIT number with class `class-2`.

**Explanation:** During RACF initialization or SETROPTS RAclist processing, a mismatch was found between classes that share a POSIT number, and the class attribute was changed for `class-1` to match the attribute in `class-2`. The named attributes, `keyword-1` and `keyword-2`, cannot be specified in classes that share a POSIT number. For example, GENERIC(DISALLOWED) and GENERIC(ALLOWED) cannot be specified in two classes that share a POSIT number (unless the classes are a grouping and member class pair).

**System action:** Processing continues and one class (`class-1`) has an updated class attribute (`keyword-2`), as specified in the message. If an installation class (static or dynamic) is sharing a POSIT number with an IBM class, the class attribute in the IBM class takes precedence. If two installation classes (static or dynamic) are sharing a POSIT number, RACF chooses the least restrictive attribute. For example, GENERIC(ALLOWED) is less restrictive than GENERIC(DISALLOWED), so RACF will choose GENERIC(ALLOWED).

**User response:** Change the definition of either `class-1` or `class-2` to have compatible attributes for classes with shared POSIT numbers. For more information about dynamic classes sharing a POSIT number, see z/OS Security Server RACF Security Administrator’s Guide. For more information about static classes sharing a POSIT number, see the ICHERCDE macro description in z/OS Security Server RACF Macros and Interfaces.

To change the attribute of a class, do one of the following tasks:

- If the class to be updated is a dynamic class, use the RALTER command to change the class attribute or POSIT number in the corresponding CDT profile.

Then issue the SETROPTS RAclist(CDT) REFRESH command to update the dynamic class descriptor table.

- If the class to be updated is a static installation-defined class, change the ICHERCDE macro invocation in module ICHRRCDE, assemble and link edit the ICHRRCDE module, and restart your system.

**Note:** If `class-1` is a dynamic class and no action is taken to change the attributes of `class-1` or `class-2`, this message is issued again during each SETROPTS RAclist(CDT) REFRESH command until the attributes are corrected.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.
RVARY command messages

ICH15001I REQUEST DENIED - RACF PERMANENTLY INACTIVE
Explanation: The RACF CVT (RCVT) indicates RACF is not active.
System action: Command processing stops.
User response: Issue this command after RACF is initialized.

ICH15002I DATASET dsname ALREADY IN REQUESTED STATE
Explanation: The user requested that the indicated data set be made active and the data set is currently active, or the user requested that the indicated data set be made inactive and the data set is currently inactive.
System action: Command processing continues with the next data set name in the list.

ICH15004I BACKUP DATASET CAN NOT BE SWITCHED; dsname IGNORED
Explanation: The user attempted to switch the indicated data set with its backup but the indicated data set is currently a backup data set.
System action: Command processing continues with the next data set name in the list.

ICH15005I PRIMARY MASTER DATASET ACTIVE; NOCLASSACT/NOTAPE OPERAND IGNORED
Explanation: The user specified either the NOCLASSACT operand or the NOTAPE operand while the primary master data set was active.
System action: RACF ignores the operand. Command processing continues with the next operand.

ICH15006I DATASET dsname HAS NO BACKUP; DATASET NOT SWITCHED
Explanation: The user attempted to switch the indicated data set with its backup but the indicated data set currently has no backup.
System action: Command processing continues with the next data set name in the list.

ICH15007I CHANGES TO RACF STATUS DENIED. OPERATOR ENTERED INCORRECT PASSWORD
Explanation: The operator entered an incorrect password in response to message ICH702A.
System action: The status of RACF remains unchanged.

User response: Provide the operator with the correct password. If you were attempting an RVARY ACTIVE, RVARY NODATASHARE, or RVARY SWITCH command, reissue the command from a console with master authority and instruct the operator to reply YES.

ICH15008I COMMAND PROCESSING TERMINATED. ERROR ENCOUNTERED DURING PASSWORD ENCRYPTION.
Explanation: To approve the user's issuance of the RVARY command, the operator must enter an installation-defined password. If RACF fails to encrypt this password at the time the operator issues it, you receive this message.
System action: Command processing stops or the command might partially complete before the error. Other messages might precede this message.
User response: Provide the operator with the correct password. If you were attempting an RVARY ACTIVE, RVARY NODATASHARE, or RVARY SWITCH command, reissue the command from a console with master authority and instruct the operator to reply YES. Report this message to your system programmer.
Programmer response: If other messages are present, examine and correct errors, then try the command again.
Problem Determination: If this message recurs, call your IBM support center.

ICH15009I ERROR ENCOUNTERED WHEN ATTEMPTING REQUESTED OPERATION, OPERATION NOT PERFORMED.
Explanation: An error occurred during RVARY processing.
System action: Command processing stops or the command might partially complete before the error. Other messages might precede this message.
User response: Report this message to your system programmer.
Programmer response: If other messages are present, examine and correct errors, then try the command again.
Problem Determination: If this message recurs, call your IBM support center.
ICH15010I ERROR WHEN INVOKING RACF DATASET ALLOCATION/DEALLOCATION OPERATION, TRY AGAIN. IF THIS PROBLEM PERSISTS, CALL OPERATOR.

Explanation: An error occurred while attempting to allocate or deallocate a RACF data set.

System action: Command processing stops or the command might partially complete before the error. Other messages might precede this message.

User response: Report this message to your operator or system programmer.

Operator response: Report this message to your system programmer.

Programmer response: If other messages are present, examine and correct errors, then try the command again.

Problem Determination: If this message recurs, call your IBM support center.

ICH15011I RVARY SWITCH DENIED. ALL REQUIRED BACKUP DATA SETS MUST BE ACTIVE BEFORE ISSUING THE SWITCH COMMAND.

Explanation: The RVARY SWITCH command was issued when one or more of the data sets to be switched was not active.

System action: The command is not processed.

Operator response: Notify the system programmer.

Programmer response: All backup data sets must be active when attempting an RVARY SWITCH command. Activate the backup data sets (using the RVARY ACTIVE command) and then switch.

ICH15013I RACF DATABASE STATUS:

Explanation: This message begins a display of RACF database status information in response to issuing the RVARY LIST command, or any RVARY command in which the NOLIST operand is not in effect.

For cases where at least one of the volumes is not shared:

ICH15013I RACF DATABASE STATUS:
ACTIVE USE NUM VOLUME DATASET SHR
-------- --- --- ------ ------- ---
YES PRIM 1 RACF01 SYS1.RACF20
NO BACK 1 RACF02 SYS1.RACF20B N
ICH15020I RVARY COMMAND HAS FINISHED PROCESSING.

For cases where all of the volumes are shared:

ICH15013I RACF DATABASE STATUS:
ACTIVE USE NUM VOLUME DATASET
-------- --- --- ------ ------- ---

ICH15014I INVALID KEYWORD ENCOUNTERED FOR RVARY

Explanation: An RVARY command was issued with an incorrect keyword specified.


ICH15017I RACF IS NOT ENABLED FOR SYSPLEX COMMUNICATIONS. DATASHARE OR NODATASHARE KEYWORDS MAY NOT BE SPECIFIED.

Explanation: The DATASHARE and NODATASHARE keywords cannot be specified when RACF is not enabled for sysplex communications.

System action: RACF does not process the command.

ICH15018I RACF DATA SHARING GROUP group-name ALREADY IN NON–DATA SHARING MODE. NODATASHARE KEYWORD MAY NOT BE SPECIFIED.

Explanation: The RACF data sharing group is already in non-data sharing mode, so RVARY NODATASHARE cannot be specified.

System action: RACF does not process the command.

ICH15019I INITIATING PROPAGATION OF RVARY COMMAND TO MEMBERS OF RACF DATA SHARING GROUP group-name [IN RESPONSE TO A REBUILD REQUEST].

Explanation: RACF is initiating the propagation of the RVARY command to the other members of the RACF data sharing group group-name. Propagation is complete when message ICH15020I is issued and subsequent RVARY commands are then processed.

System action: The command is propagated.

ICH15020I RVARY COMMAND [INITIATED IN RESPONSE TO THE REBUILD REQUEST] HAS FINISHED PROCESSING.

Explanation: The RVARY command processing has completed. If this message is preceded by other messages, refer to those messages for appropriate action. Subsequent RVARY commands can now be processed.

System action: RACF continues operation.

Operator response: RVARY processing was not
completely successful if this message is preceded by any of the following messages:

ICH15009I  IRRX003A
ICH15010I  IRRX009I
ICH15011I  IRRX010I
ICH15021I  IRRX011A
ICH15022I  IRRX012I
ICH15023I  IRRX013A
ICH15024I
ICH15025I
ICH15026I

Refer to those messages for further action.

ICH15021I  UNABLE TO OBTAIN SERIALIZATION FOR THE REQUESTED COMMAND. THE COMMAND IS NOT PERFORMED.

Explanation: RACF was unable to obtain serialization to perform the requested command.

System action: RACF does not process the command.

User response: Report this message to your system programmer.

System programmer response: Check the system log for serialization-related messages to determine and correct the problem.

ICH15022I  ONE OR MORE MEMBERS OF THE RACF DATA SHARING GROUP FAILED TO PROCESS THE PROPAGATED RVARY COMMAND.

Explanation: RACF is enabled for sysplex communication and propagated the command to the other members of the RACF data sharing group. However, one or more members of the group failed to process the command as expected.

System action: Command propagation completes. One or more members had a processing error.

User response: Report this message to your system programmer.

System programmer response: Check the system log for IRRX006I messages. If found, these messages identify the members who experienced the failure. Obtain the system logs for each failing member to determine additional RACF messages that might have been issued. RVARY LIST may also be used to determine if the status of the failing members is different from what was expected. If you do not find any IRRX006I messages, an XCF failure might have occurred during processing. Any member that leaves the RACF data sharing group because of this failure issues the ICH501I message.

ICH15023I  ERROR OCCURRED WHILE INVOKING RVARY COMMAND.

Explanation: An internal error occurred during an attempt to process an RVARY command.

System action: RACF does not process the command.

User response: Report this message to your system programmer.

System programmer response: Save dumps and the system log. Contact your IBM support center. An IPL might be necessary.

ICH15024I  RACF IS PROCESSING A PRIOR RVARY COMMAND. [RE-ISSUE THE COMMAND.]

Explanation: RACF has not completed processing of a prior RVARY command.

System action: RACF does not process the command.

User response: For rebuild, issue the RVARY NODATASHARE command followed by an RVARY DATASHARE command. Otherwise, reissue the original RVARY command. If this message persists, contact your system programmer.

System programmer response: Use the MVS DUMP command to obtain a dump of the Master, RACFDS, and RACF subsystem address spaces and call your IBM support center. An IPL might be necessary.

ICH15025I  THE RVARY COMMAND WAS NOT PROCESSED BY ANY MEMBER OF THE RACF DATA SHARING GROUP.

Explanation: RACF is enabled for sysplex communication and attempted to propagate the command to the other members of the RACF data sharing group. However, none of the members of the group processed the command. If RVARY propagation was interrupted by an XCF failure, it is possible that some members of the RACF data sharing group might have quiesced activity against the RACF database in preparation for processing the command. These members cannot use the RACF database until the command is reissued and processing is complete.

System action: RACF does not process the command.

User response: Report this message to your system programmer.

System programmer response: Check the system log for additional information, such as XCF failures, IRRX006I messages, or other related RACF messages. Correct the problem and reissue the command.
ICH15026I  A SEVERE ERROR OCCURRED DURING THE PROPAGATION OF THE RVARY COMMAND.

Explanation: RACF detected a severe error while attempting to propagate an RVARY command.

System action: The RACF data sharing group has attempted to process the command, but this member experienced a severe error. In order to prevent damage to the RACF database and to ensure that other members of the RACF data sharing group are not affected by the error, this member has entered permanent failsoft mode and has been removed from the group.

User response: Report this message to your system programmer.

System programmer response: Check the system log for additional information. Save dumps and the system log. See the MVS documentation on XCF failures. If necessary, contact your IBM support center. An IPL is required to return this member to an active state.

ICH15027I  RVARY COMMAND REJECTED. ROUTE IS ONLY ALLOWED FOR RVARY LIST. RE-ISSUE COMMAND TO A SINGLE SYSTEM ONLY.

Explanation: The RVARY command was prefixed with the MVS ROUTE command, directing the command to multiple members of the RACF data sharing group. This is allowed only for RVARY LIST, with no additional RVARY keywords specified. If you reissue the RVARY command to a single member only, RACF propagates the command to the other members of the group.

System action: RACF does not process the command.

Operator response: Reissue the command to a single member.

ICH15028I  MVS RELEASE LEVEL IS NOT AT LEAST RELEASE 5.1. DATASHARE OR NODATASHARE KEYWORDS CANNOT BE SPECIFIED.

Explanation: All members of the RACF data sharing group must be at MVS 5.1 or above for an RVARY DATASHARE or RVARY NODATASHARE command to function. This message indicates that the member to which the command was issued was not at the sufficient level.

System action: RACF does not process the command.

System programmer response: If data sharing is wanted, all the members of the RACF data sharing group must be upgraded to MVS 5.1 or above.

ICH15029I  THIS MEMBER OF THE RACF DATA SHARING GROUP IS IN READ-ONLY MODE. THE SWITCH KEYWORD MAY NOT BE SPECIFIED.

Explanation: This member of the RACF data sharing group is in read-only mode, so RVARY SWITCH cannot be specified.

System action: RACF does not process the command.

User response: Reissue the command from a member of the RACF data sharing group that is not in read-only mode. If all members are in read-only mode, issue the RVARY NODATASHARE command, followed by the RVARY SWITCH command.

ICH15030I  INITIATING AUTOMATIC DATA SET SWITCH TO BACKUP FOR data-set-name.

Explanation: RACF has detected that the device that the primary RACF data set indicated in the message has been varied offline. To prevent additional I/O errors, an RVARY SWITCH to the backup data set has been initiated.

System action: RVARY processing continues.

ICH15031I  ICHEVENTY TYPE ERROR AGAINST PROFILE PROFILE-NAME IN CLASS CLASS-NAME ON THE DATABASE WITH MASTER DATA SET dsname. HEX RC=RC, AND REASON=REASON

Explanation: The ICHEVENTY encountered a failing return or reason code where:
- Type is the type of ICHEVENTY (‘NEXT’ or ‘ALTER’)
- Profile is the profile name
  - for ICHEVENTY ALTER the profile name is 9 to 16 characters in length.
  - for ICHEVENTY NEXT a profile name might be 247 characters in length. A maximum of the first 20 characters of the profile name is presented in the message.
- Class is the General Resource class
- The dsname indicates the database

If there is an ICHEVENTY NEXT failure, then because the IRRPLEX_ profiles are used to shield the database from corruption caused by incorrect database sharing, there might be a gap in that analysis.

If there is an ICHEVENTY ALTER failure, then because the IRRPLEX_ profiles are used to shield the database from corruption caused by incorrect database sharing, there might be a gap in a future analysis.

System action: In both cases processing continues.

Operator response: Contact your system programmer.
If the RVARY DATASHARE, NODATASHARE, or ACTIVE command is successful then:

If there is an ICHEINTY ALTER failure, issue an RLIST command on the named profile. If this is successful issue an RVARY LIST command:

• If the RVARY LIST command indicates that the system is in data sharing mode, issue an RALTER command on the named profile and enter “DATA SHARING MODE” into the APPLDATA field.

• If the RVARY LIST command indicates that the system is in read-only mode and another system is using the database in data sharing mode, issue an RALTER command from that system on the named profile and enter “DATA SHARING MODE” into the APPLDATA field.

• If the RVARY LIST command does not indicate data sharing mode or read-only mode, issue an RALTER command on the named profile and enter “NON-DATA SHARING MODE” into the APPLDATA field.

If there is an ICHEINTY NEXT failure, issue a SEARCH command. For example:

SEARCH CLASS(GXFACILI) MASK(IRRPLEX_)

If there are still failures, issue an RDELETE command on the profile. If this is successful, re-create the profile by using the RDEFINE command, and either enter “data sharing mode” or “non-data sharing mode” in the APPLDATA field, as determined by the RVARY command.

If there is an ICHEINTY NEXT failure, then because the IRRPLEX_ profiles are used to shield the database from corruption caused by incorrect database sharing, there might be a gap in that analysis. The database can become corrupted if:

• The RACF database is shared with systems that are outside the global resource serialization complex, and any of the sharing systems are in data sharing mode. Or,

• There are systems within the global resource serialization complex that are in data sharing mode, and any other sharing systems are in non-data sharing mode.

You can issue an RVARY list command to determine the database names and volsers. This also indicates if the system is in data sharing mode. If the RACF database is incorrectly shared, run IRRUT200 against each data set and either move all sharing sysplexes out of data sharing mode into non-data sharing mode (RVARY NODATASHARE), or change your database sharing configuration. If the database is already corrupted, either restore an archived backup of the database, or contact your IBM support center.

If the message indicates that the ICHEINTY NEXT was run against the backup database, and you did not receive this message for the primary database, then if the backup database is intended to be the same as the primary database, resynchronize the primary and the backup databases by using IRRUT200 PARM=ACTIVATE.

Note: Ensure that the database you are using as the backup database is the correct database to be using with your primary database. The IRRUT200 PARM=ACTIVATE will overlay all the data within the specified backup data set. See z/OS Security Server RACF System Programmer’s Guide for more information about IRRUT200.

If the problem persists, contact your IBM support center.

Do not use RRSF to propagate the RDEFINE, RALTER, and RDELETE commands to other databases. If automatic command direction is enabled for the GXFACILI class, use the ONLYAT operand (on the RALTER, RDEFINE, and RDELETE commands) when you change IRRPLEX_sysplex-name profiles to prevent this propagation. You must use ONLYAT whether you are altering, creating, or deleting the class GXFACILI IRRPLEX_sysplex-name profiles on a local or remote node.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

ICH15032I RACDEF DEFINE ERROR AGAINST PROFILE PROFILE-NAME IN CLASS CLASS-NAME ON THE DATABASE WITH MASTER DATA SET DSNAME. HEX RC=RC, AND REASON=REASON

Explanation: RACDEF encountered a failing return code or reason code. After the successful completion of the RVARY function, the creation of the named profile encountered a failure.

• Profile is the profile name
• Class is the General Resource class
• Dsname indicates the database

Because the IRRPLEX_ profiles are used to shield the database from corruption caused by incorrect database sharing, there might be a gap in a future analysis.

System action: The RVARY command continues.

Operator response: Contact your system programmer.

System programmer response: Issue an RVARY LIST command:
If the RVARY LIST command indicates that the system is in data sharing mode, issue an RDEFINE command on the named profile and enter “DATA SHARING MODE” into the APPLDATA field.

If the RVARY LIST command indicates that the system is in read-only mode and another system is using the database in data sharing mode, issue an RDEFINE command from that system on the named profile and enter “DATA SHARING MODE” into the APPLDATA field.

If the RVARY LIST command does not indicate data sharing mode or read-only mode, issue an RDEFINE command on the named profile and enter “NON-DATA SHARING MODE” into the APPLDATA field.

Do not use RRSF to propagate the RDEFINE, RALTER, and RDELETE commands to other databases. If automatic command direction is enabled for the GXFACILI class, use the ONLYAT operand (on the RALTER, RDEFINE, and RDELETE commands) when you change IRRPLEX_sysplex-name profiles to prevent this propagation. ONLYAT must be used whether you are altering, creating, or deleting the class GXFACILI IRRPLEX_sysplex-name profiles on a local or remote node.

If the problem persists, run IRRUT200 (specifying INDEX FORMAT and MAP ALL in the SYSIN DD) against the data set within the database that contains the named profile, and contact your IBM support center.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

**ICH15033A**

**IF ANY SYSTEM IS USING THE DATABASE WITH MASTER DATASET DSNAMES IN DATA SHARING MODE, AND ANY OTHER SYSTEM CONCURRENTLY USES IT IN NON-DATA SHARING MODE, DATABASE CORRUPTION WILL RESULT. PROFILE PROFILE-NAME IN CLASS CLASS-NAME INDICATES THAT THIS DATABASE WAS LAST USED IN DATA SHARING MODE, BUT IT IS NOW TO BE USED IN NON-DATA SHARING MODE. IF THE DATABASE IS NOT BEING USED BY ANOTHER SYSTEM IN DATA SHARING MODE, SPECIFY ‘CONTINUE’. OTHERWISE SPECIFY ‘CANCEL’.

**Explanation:** The APPLDATA field of one or more IRRPLEX_sysplex-name profiles indicates data sharing mode. However, this system is in non-data sharing mode. The data sharing mode indicators within the IRRPLEX_profiles are incompatible with the non-data sharing mode of this environment.

The ICH15041A WTOR is issued after this message to obtain a response.

Specify CONTINUE if:

- the named profile is for this sysplex, and the named database is now to be used in non-data sharing mode.

- you have copied the database from an environment that shared the database with another sysplex in data sharing mode, but which is no longer true for this environment.

- the sysplex was renamed, and is no longer in data sharing mode.

- one or more IRRPLEX_profiles were manually altered or created incorrectly:
  - the profile name indicates a sysplex that is not sharing the database.
  - the APPLDATA field indicates data sharing mode (anything that begins with a “D”), but the system is not in data sharing mode

- an automated update of one or more IRRPLEX_profiles failed.

Specify CANCEL if:

- the named profile is for this sysplex, the database is being used by this sysplex in data sharing mode, the system is not enabled for RACF sysplex communication, but you must be in RACF sysplex communication. Update the data set name table (ICHRD5N) to request RACF sysplex communication and data sharing mode, and then re-IPL the system.

- the profiles are correct, the database is being used by this sysplex, or another sysplex, in data sharing mode, and you must not use the database. Update the data set name table (ICHRD5N) to request a different database, and then re-IPL the system.

**System action:** The system waits for the operator’s reply.

**Operator response:** Respond to the ICH15041A message or contact your system programmer.

**System programmer response:** If the identified database is being used in data sharing mode by another system, the database becomes corrupted in the following situations:

- The other system is in another sysplex.

- The other system is in this sysplex, but this system is not enabled for RACF sysplex communication (which would have forced this system to use the databases and mode of the IRRXCF00 RACF sysplex communication group).

You must specify CANCEL to protect the database.

**Notes:**

1. If the other system is in another sysplex, either change the data set name table (ICHRD5N) to use
a different database, and then re-IPL the system, or issue an RVARY NODATASHARE command from the other sysplex.

2. If the other system is in this sysplex, but is not being used in data sharing mode, change the data set name table (ICHRDSNT) to request RACF sysplex communication or data sharing mode, or both, and then re-IPL the system. This causes the IRRXCF00 group to be joined and the RACF sysplex communication group data set name table, which must be in the correct mode, to be used.

If the identified database is not being used in data sharing mode, specify CONTINUE. After the RVARY, use the RDELETE or RALTER command on the IRRPLEX_sysplex-name profiles as appropriate. The IRRPLEX_sysplex-name profile for this sysplex is updated automatically during the RVARY processing.

If the message indicates the backup database, and you did not receive this message for the primary database, then if the backup database is intended to be the same as the primary database, and you were able to specify ‘CONTINUE’ to this message, resynchronize the primary and the backup databases using ‘IRRUT200 PARM=ACTIVATE’.

Note: Ensure that the database you are using as the backup database is the correct database to be using with your primary database. The ‘IRRUT200 PARM=ACTIVATE’ overlays all the data within the specified backup data set. See z/OS Security Server RACF System Programmer’s Guide for more information about IRRUT200.

If the problem persists, contact your IBM support center.

Do not use RRSF to propagate the RDEFINE, RALTER, and RDELETE commands to other databases. If automatic command direction is enabled for the GXFACILI class, use the ONLYAT operand (on the RALTER, RDEFINE, and RDELETE commands) when you change IRRPLEX_sysplex-name profiles to prevent this propagation. ONLYAT must be used whether you are altering, creating, or deleting the class GXFACILI IRRPLEX_sysplex-name profiles on a local or remote node.

Destination: Descriptor code is 2. Routing code is 1.
Contact your system programmer.

**System programmer response: RVARY ACTIVE:**

If the identified database is being used by another system, which is in another sysplex, and this system is in data sharing mode, the database becomes corrupted. You must specify CANCEL to protect the database.

If the identified database is not being used in data sharing mode, specify CONTINUE. After the RVARY, use the RDELETE or RALTER command on the IRRPLEX_sysplex-name profiles as appropriate. The IRRPLEX_sysplex-name profile for this sysplex is updated automatically during the RVARY processing.

If the message indicates the backup database, and you did not receive this message for the primary database, then if the backup database is intended to be the same as the primary database, and you were able to specify ‘CONTINUE’ to this message, resynchronize the primary and the backup databases by using 'IRRUT200 PARM=ACTIVATE'.

**Note:** Ensure that the database you are using as the backup database is the correct database to be using with your primary database. The ICH15037I message indicates the backup database, and you did not receive this message for the primary database. If the backup database is intended to be the same as the primary database, and you were able to specify 'CONTINUE' to this message, resynchronize the primary and the backup databases by using 'IRRUT200 PARM=ACTIVATE'.

If the problem persists, contact your IBM support center.

Do not use RRSF to propagate the RDEFINE, RALTER, and RDELETE commands to other databases. If automatic command direction is enabled for the GXFACILI class, use the ONLYAT operand (on the RALTER, RDEFINE, and RDELETE commands) when you change IRRPLEX_sysplex-name profiles to prevent this propagation. ONLYAT must be used whether you are altering, creating, or deleting the class GXFACILI IRRPLEX_sysplex-name profiles on a local or remote node.

**RVARY DATASHARE:**

Refer to the RVARY ACTIVE system programmer response above.

If the GXFACILI IRRPLEX_sysplex-name profiles, which are not for this sysplex, are extraneous, delete them before reissuing the RVARY DATASHARE.

If the GXFACILI IRRPLEX_sysplex-name profiles are correct and this database is being used by another system, which is in another sysplex, the database becomes corrupted.

If this system must enter data sharing mode, stop sharing the database with systems in other sysplexes.

Then delete the now extraneous profiles and reissue the RVARY DATASHARE command.

**Destination: RVARY ACTIVE:**

 Descriptor code is 2. Routing code is 1.

**RVARY DATASHARE:**

Descriptor code is 11. Routing code is 1.

ICH15037I IN CLASS GXFACILI, AN IRRPLEX PROFILE WAS ENCOUNTERED ON THE DATABASE WITH MASTER DATA SET DSNAME, BUT THE SYSPLEX NAME PORTION OF THE PROFILE NAME WAS GREATER THAN 8 CHARACTERS. DATABASE SHARING CHECKS HAVE IGNORED PROFILE IRRPLEX_SYSPLEX-NAME.

**Explanation:** For each unique sysplex name there might exist one IRRPLEX profile. These profiles contain APPLDATA information, and are used by the routines, which protect the database from being used in an incorrect sharing environment, to prevent database corruption. A(sysplex name is limited to eight characters in length. No information from this profile is considered by the anti-corruption scheme.

A maximum of the first 20 characters of the profile name is presented in the message.

**System action:** The system continues processing.

**Operator response:** Contact your system programmer.

**System programmer response:** IRRPLEX_sysplex-name profiles are used by the routines that protect the database from bad sharing. If the names of profiles in the GXFACILI class begin with “IRRPLEX_”, they might remain if the environment has other uses for them, and this message can be ignored.

If a sysplex, which runs at code levels less than in z/OS R10, shares this database (RVARY LIST from the security console), and you manually created the profile to ensure that the code, which shields the database from bad sharing, gets more pertinent information, you must issue an RDELETE command on the profile and reissue the command with a valid 8-character sysplex name.

Systems running release z/OS R10 or later, automatically create and maintain these profiles.

If the message indicates the backup database, and you did not receive this message for the primary database, then if the backup database is intended to be the same as the primary database, resynchronize the primary and the backup databases using 'IRRUT200 PARM=ACTIVATE'.

**Note:** Ensure that the database you are using as the backup database is the correct database to be using with your primary database. The
"IRRUT200 PARM=ACTIVATE" overlays all the data within the specified backup data set. See z/OS Security Server RACF System Programmer’s Guide for more information about IRRUT200.

If the problem persists, contact your IBM support center.

Do not use RRSF to propagate the RDEFINE, RALTER, and RDELETE commands to other databases. If automatic command direction is enabled for the GXFACILI class, use the ONLYAT operand (on the RALTER, RDEFINE, and RDELETE commands) when you change IRRPLEX_sysplex-name profiles to prevent this propagation. ONLYAT must be used whether you are altering, creating, or deleting the class GXFACILI IRRPLEX_sysplex-name profiles on a local or remote node.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

ICH15038I IN CLASS GXFACILI, A PROFILE IRRPLEX_SYSPLEX-NAME WAS ENCOUNTERED ON THE DATABASE WITH MASTER DATA SET DSNAME. ITS APPLDATA IS NOT A RECOGNIZED VALUE.

Explanation: The APPLDATA field might indicate the RACF mode. If the profile is updated automatically, it contains “NON-DATA SHARING MODE” or “DATA SHARING MODE”. If the APPLDATA field is set manually by using RDEFINE or RALTER, the following values indicate the mode:

- If the first character is “N” it is an indication of non-data sharing mode.
- If the first character is “D” it is an indication of data sharing mode.

This APPLDATA field of the profile did not provide information for the support that protects the database from bad sharing.

System action: The system continues processing.

Operator response: Contact your system programmer.

System programmer response: It is assumed that the IRRPLEX_sysplex-name profile has been updated manually, and that the APPLDATA field has been updated incorrectly. An APPLDATA value that is not valid has no influence over the support to detect incorrect database sharing.

If you attempted to manually create a profile for a sysplex that shares the RACF database, but which is running at a level of RACF without the support required to detect incorrect database sharing, you entered incorrect APPLDATA. Systems that run release z/OS R10 or later, on a particular sysplex, automatically create and maintain these sysplex related profiles.

If the profile is for the sysplex that received this message, and the RVARY command completed in non-data sharing mode or data sharing mode, the APPLDATA is updated automatically. If the profile is not for this sysplex, you must issue an RALTER command and update the APPLDATA field of the named profile with a recognized value.

If the message indicates the backup database, and you did not receive this message for the primary database, then if the backup database is intended to be the same as the primary database, resynchronize the primary and the backup databases using "IRRUT200 PARM=ACTIVATE".

Note: Ensure that the database you are using as the backup database is the correct database to be using with your primary database. The "IRRUT200 PARM=ACTIVATE" will overlay all the data within the specified backup data set. See z/OS Security Server RACF System Programmer’s Guide for more information about IRRUT200.

If the problem persists, contact your IBM support center.

Do not use RRSF to propagate the RDEFINE, RALTER, and RDELETE commands to other databases. If automatic command direction is enabled for the GXFACILI class, use the ONLYAT operand (on the RALTER, RDEFINE, and RDELETE commands) when you change IRRPLEX_sysplex-name profiles to prevent this propagation. ONLYAT must be used whether you are altering, creating, or deleting the class GXFACILI IRRPLEX_sysplex-name profiles on a local or remote node.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

ICH15041E THE RESPONSE WAS UNRECOGNIZED. RESPECIFY RESPONSE.

Explanation: A WTOR has been issued, and an unrecognized response was proffered by the operator.

System action: The WTOR is reissued.

Operator response: An unexpected response was made to the ICH15041A WTOR to get a response to the scenario identified by one of the following WTOs: ICH15033A, ICH15034A, or ICH15042A. Ensure that you use a complete keyword that the specific WTO is expecting.

Destination: Descriptor code is 4. The message is only sent to the console ID that replied incorrectly to ICH15041A.
ICH15041A • ICH15042A

ICH15041A VALID RESPONSES ARE ‘CONTINUE’ OR ‘CANCEL’

Explanation: One of the following WTOs: ICH15033A, ICH15034A, or ICH15042A has been issued and this WTO is requesting a response by the operator.

System action: If the response is one of the expected keywords, it is accepted. If the response is not one of the expected keywords, ICH15040I is issued, and then ICH15041A is reissued.

Operator response: Respond to the scenario proffered by one of the following WTOs: ICH15033A, ICH15034A, or ICH15042A. Ensure that you use a complete keyword that the specific WTO is expecting.

Destination: Descriptor code is 7. Routing code is 1.

If the response is not one of the expected keywords, and the message is reissued, then it is only sent to the console ID that replied incorrectly to the previous ICH15041A.

ICH15042A IF ANY SYSTEM IS USING THE DATABASE WITH MASTER DATA SET DSNNAME IN DATA SHARING MODE, AND ANY OTHER SYSTEM CONCURRENTLY USES IT IN NON-DATA SHARING MODE, DATABASE CORRUPTION WILL RESULT. YOU ARE RVARYING INTO A DATA SHARING MODE ENVIRONMENT. PROFILE PROFILE-NAME IN CLASS CLASS-NAME INDICATES THAT THIS DATABASE WAS LAST USED IN NON-DATA SHARING MODE, BUT IT IS NOW TO BE USED IN DATA SHARING MODE. IF THE DATABASE IS BEING USED BY ANOTHER SYSTEM NOT ENABLED FOR RACF SYSPLEX COMMUNICATION SPECIFY ‘CANCEL’. OTHERWISE SPECIFY ‘CONTINUE’.

Explanation: The APPLDATA field of the IRRPLEX_sysplex-name profile, for this sysplex, indicates non-data sharing mode. This system is currently changing to a data sharing mode environment. A system in data sharing mode cannot safely share a database with a system that is not in data sharing mode.

If the sysplex is changed into data sharing mode by a system running a release previous to z/OS R10, the automatic update, which indicates the new mode in the IRRPLEX_sysplex-name profile, did not happen, and it is normal to receive this message.

To ensure that your database avoids corruption you must determine if the databases are being shared by other sysplex members that are not enabled for RACF sysplex communication. Systems that are enabled for RACF sysplex communication are members of the XCF IRRXCF00 group.

First determine which systems are sysplex members, but not IRRXCF00 group members. To display sysplex members, enter the following command from the master console:

D XCF, SYSPLEX

To display group members, enter the following command from the master console:

D XCF, GROUP, IRRXCF00

Next issue an RVARY LIST command from the systems in the sysplex that are not IRRXCF00 group members. This indicates if the systems are using the same databases as the systems within the group. If there are systems using the same databases, this is because either:

- The data set name table (ICHRDSNT) of the other systems sharing the databases did not specify RACF sysplex communication during IPL (the databases are used in the same mode as the group). Or,
- This sysplex should not be in data sharing mode. Or,
- One of the systems has specified an incorrect RACF database in the data set name table (ICHRDSNT)

The ICH15041A WTO is issued after this message to obtain a response.

Specify CONTINUE if:

- there are no systems in this sysplex, which are not enabled for RACF sysplex communication, that are using this database.

Specify CANCEL if:

- the profile is correct, and you must not use the database in data sharing mode.

System action: The system waits for the operator’s reply.

Operator response: Respond to the ICH15041A message or contact your system programmer.

System programmer response: If the database is being used by another system that is not enabled for RACF sysplex communication (which implies that it can never change out of non-data sharing mode), and this system is in data sharing mode, the database will become corrupted. You must specify CANCEL to protect the database. You can then either:

- Issue an RVARY NODATASHARE from the system in data sharing mode, before retrying the RVARY ACTIVE. Or,
- For systems using the database that are not enabled for RACF sysplex communication, but must be using the same database, update the data set name table (ICHRDSNT), and then reIPL the updated systems.
If the identified database is not being used by another system in this sysplex, which is not enabled for RACF Sysplex Communication mode, specify CONTINUE. After the RVARY, the IRRPLEX\_sysplex-name profile for this system is updated.

If the message indicates the backup database, and you did not receive this message for the primary database, then if the backup database is intended to be the same as the primary database, and you were able to specify 'CONTINUE' to this message, resynchronize the primary and the backup databases using "IRRUT200 PARM=ACTIVATE".

**Note:** Ensure that the database you are using as the backup database is the correct database to be using with your primary database. The "IRRUT200 PARM=ACTIVATE" overlays all the data within the specified backup data set. See the z/OS Security Server RACF System Programmer’s Guide for more information about IRRUT200. If the problem persists, contact your IBM support center.

Do not use RRSF to propagate the RDEFINE, RALTER, and RDELETE commands to other databases. If automatic command direction is enabled for the GXFACILI class, use the ONLYAT operand (on the RALTER, RDEFINE, and RDELETE commands) when you change IRRPLEX\_sysplex-name profiles to prevent this propagation. ONLYAT must be used whether you are altering, creating, or deleting the class GXFACILI IRRPLEX\_sysplex-name profiles on a local or remote node.

**Destination:** Descriptor code is 2. Routing code is 1.
ALTGROUP command messages

ICH20002I NOT AUTHORIZED TO ALTER
group-name
Explanation: You do not have sufficient authority to alter the group indicated in the message.
System action: Command processing stops.
User response: See your RACF security administrator.

ICH20003I NOT AUTHORIZED TO SPECIFY OWNER
Explanation: You do not have sufficient authority to specify the OWNER operand.
System action: Processing continues with the owner field unchanged.
User response: See your RACF security administrator.

ICH20004I ERROR FOUND IN GROUP TREE STRUCTURE
Explanation: An inconsistency or error was found in the group tree structure while processing the ALTGROUP command.
System action: Command processing stops.
User response: Use the LISTGRP command to list groups in the superior group tree structure, looking in particular for disagreements between superior groups and subgroups.

ICH20005I INSUFFICIENT AUTHORITY TO [SUPERIOR GROUP OF] group-name
Explanation: You do not have sufficient authority to change the superior group indicated in the message.
System action: Command processing stops.
User response: See your RACF security administrator.

ICH20006I xxxxxxxx CANNOT BE A SUPERIOR GROUP OF yyyyyyy
Explanation: The command requested that group xxxxxxxx be made the superior group of yyyyyyy. However, group yyyyyyy is already above group xxxxxxxx in the group hierarchy and the result would be a circular definition that is invalid.
System action: The subgroup list for group xxxxxxxx is not changed. Command processing stops.

ICH20007I {TERMUACC | NOTERMUACC} NOT ALTERED FOR GROUP group-name
Explanation: An error occurred while altering the TERMUACC or NOTERMUACC operand for the group indicated in the message. The TERMUACC and NOTERMUACC indicators in the group profile and connect entries are not updated.
System action: Command processing continues with the next operand.

ICH20008I {TERMUACC | NOTERMUACC} NOT ALTERED FOR {USER userid | ANY USERS}
Explanation: An error occurred during one of the following processes:
• Retrieving the access list of all users connected to the group (indicated by ANY USERS)
• Altering the TERMUACC or NOTERMUACC indicator in the connect profile for user userid
System action: The TERMUACC or NOTERMUACC indicator in the group profile was altered to the value specified on the command. If the error occurred while retrieving the access list, command processing stops. If the error occurred while altering a connect profile for user userid, command processing continues with the next user ID in the access list.

ICH20009I group-name NOT ALTERED, PROGRAMMING LIMIT EXCEEDED
Explanation: While searching the index structure for the superior group of the group specified, more than 398 superior groups were found. This exceeds the RACF command limit.
System action: RACF ignores the SUBGROUP operand. Command processing continues with the next operand.

ICH20010I NOT AUTHORIZED TO ISSUE ALTGROUP
Explanation: One of the following conditions is true:
• RACF is inactive.
• You are not defined to RACF and cannot issue RACF commands.
• You are not defined to RACF with sufficient authority to issue this command.
System action: Command processing stops.
User response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or the authority required to issue the indicated
ICH20011I    COMMAND ENDED DUE TO ERROR
Explanation:  An ESTAE recovery environment cannot be established.
System action:  Command processing stops.
User response:  Report this message to your system programmer. Include the following information:
   • The message ID
   • The exact wording of the command you entered
   • The date and time you entered the command
System programmer response:  Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

ICH20012I    RECOVERY UNSUCCESSFUL
Explanation:  As issued, the ALTGROUP command began to update more than one profile in the RACF database. However, a system or RACF failure occurred during command processing.
System action:  To prevent discrepancies among profiles, RACF attempted to back out any changes already made to profiles. However, not all changes can be backed out. This message follows message ICH20013I.
User response:  Report this message and the exact text of message ICH20013I to your system programmer.
Problem Determination: The RACF utility programs might be needed to correct the RACF database.

ICH20013I    group-name NOT ALTERED
-or-
GROUP(S) NOT ALTERED
Explanation:  An error occurred during ALTGROUP command processing.
System action:  The group indicated in the message was not altered.

ICH20014I    OWNER NOT ALTERED FOR group-name
Explanation:  An error occurred while processing the owner field specified in the OWNER operand.
System action:  RACF does not alter the owner field. Command continues processing with the next operand.

ICH20015I    SUPGROUP NOT ALTERED FOR group-name
Explanation:  An error occurred while processing the superior group field specified in the SUPGROUP operand.
System action:  The superior group field is not altered and the command continues processing with the next operand.

ICH20016I    NOT AUTHORIZED TO SPECIFY THE DATA OR NODATA KEYWORDS
Explanation:  You do not have sufficient authority to alter the installation-defined data in the group profile.
System action:  Command processing stops.
User response:  See your RACF security administrator.

ICH20017I    NOT AUTHORIZED TO SPECIFY THE MODEL OR NOMODEL KEYWORDS
Explanation:  You do not have sufficient authority to specify the MODEL or NOMODEL operand on the ALTGROUP command.
System action:  Command processing stops.
User response:  See your RACF security administrator.

ICH20018I    WARNING, UNABLE TO LOCATE THE MODEL PROFILE FOR dsname
Explanation:  You have specified a model profile data set name that cannot be found on the RACF database. For modeling to be effective for this data set name, a data set profile must first be created.
System action:  RACF adds the data set name you specified to the group profile in anticipation that profile information for this name is completed (by using the ADDSD command) at a later time.
RACF continues to process the ALTGROUP command.

ICH20019I    UNABLE TO LOCATE group-name
Explanation:  The group indicated in the message cannot be found in the RACF database.
System action:  Command processing continues with the next group name in the list.

ICH20020I    OWNER-GROUP AND SUPERIOR GROUP MUST BE THE SAME FOR GROUP group-name
Explanation:  When the owner of a group is another group, the owning group and the superior group must be the same. This message is followed by message ICH20014I or message ICH20015I, or both.
ICH20021I  PROFILE UNCHANGED. NOT
AUTHORIZED TO ALTER SEGMENT
FOR GROUP group-name

Explanation: You are not authorized to change the
segment for the specified group.

System action: Command processing ends with no
update to the group profile.

User response: See your RACF security administrator
for authority to the segment of this group profile.

RACF Security Administrator Response: You can use
field-level access checking to allow this user to add
segment information. For a description of field-level
access checking, see z/OS Security Server RACF Security
Administrator’s Guide.

ICH20022I  DFP SEGMENT NOT ALTERED FOR
GROUP group-name

Explanation: You are not authorized to change the
DFP segment for the specified group.

System action: Command processing stops with no
update to the group profile.

User response: See your RACF security administrator
for authority to the DFP segment of this group profile.

RACF Security Administrator Response: You can use
field-level access checking to allow this user to add
DFP segment information. For a description of
field-level access checking, see z/OS Security Server
RACF Security Administrator’s Guide.
ALTUSER command messages

ICH21001I COMMAND ENDED DUE TO ERROR UNABLE TO PROMPT FOR OIDCARD

Explanation: You specified the OIDCARD operand, but TSO/E was unable to prompt you to enter the operator identification card.

System action: Command processing stops.

User response: Be sure that you are executing the command in the foreground and in prompt mode.

ICH21002I COMMAND ENDED DUE TO ERROR UNABLE TO ESTABLISH ESTAE

Explanation: An ESTAE recovery environment cannot be established.

System action: Command processing stops.

User response: Report this message to your system programmer. Include the following information:
- The message ID
- The exact wording of the command you entered
- The date and time you entered the command

System programmer response: Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

ICH21003I COMMAND ENDED DUE TO ERROR PUTGET ERROR RETURN CODE IS xx

Explanation: You specified the OIDCARD operand, but the TSO/E PUTGET service routine failed with a return code indicated by xx while trying to read the operator identification card. For an explanation of the return code, see z/OS TSO/E Programming Services For the order number of the documentation you need, see z/OS TSO/E General Information.

ICH21004I {userid | DFLTGRP | OWNER | USER} NOT ALTERED

Explanation: An error occurred during RACF processing.

System action: If a user ID appears in the message, the user profile was not changed. If USER appears, the error occurred before a particular user ID can be determined. Otherwise, the DFLTGRP or OWNER fields were not altered.

User response: One of the following conditions is true:
- If DFLTGRP appears in the message, the user specified on the ALTUSER command was not already connected to the group specified on the DFLTGRP operand. Use the CONNECT command to connect the user to the group (with the wanted group authority), then issue the ALTUSER command with DFLTGRP specified again.
- If OWNER appears in the message, there is no profile (user or group, as appropriate) for the owner specified on the ALTUSER command.

ICH21005I NOT AUTHORIZED TO SPECIFY operand, OPERAND IGNORED

Explanation: You do not have sufficient authority to specify the indicated operand.

System action: RACF ignores the operand and continues processing with the next operand.

User response: See your RACF security administrator.

ICH21006I AUTHORITY SPECIFIED GREATER THAN THE COMMAND USER

Explanation: You have CONNECT authority and cannot specify JOIN authority. The other operands were modified.

User response: See your RACF security administrator.

ICH21007I EXPIRED/NOEXPIRED OPERAND IGNORED

Explanation: You specified the EXPIRED or NOEXPIRED operand but the PASSWORD or the PHRASE operand was specified on the command. EXPIRED and NOEXPIRED are valid only if they are specified with the PASSWORD or PHRASE operand.

System action: RACF ignores the operand and continues command processing with the next operand.

ICH21008I NOT AUTHORIZED TO SPECIFY CLAUTH/NOCLAUTH FOR {USER, TAPEVOL, DASDVOL, TERMINAL}, CLASS IGNORED

Explanation: You do not have sufficient authority to specify the CLAUTH or NOCLAUTH operands for the indicated class.

System action: RACF ignores the class and continues command processing with the next class specified.

User response: See your RACF security administrator.

ICH21009I UNABLE TO LOCATE userid

Explanation: The indicated user ID cannot be found in the RACF database.

System action: Command processing stops.
ICH21010I NOT AUTHORIZED TO ISSUE ALTUSER

Explanation: One of the following conditions is true:
- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System action: Command processing stops.

User response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or the authority required to issue the indicated command, see z/OS Security Server RACF Command Language Reference.

ICH21011I [AUTHORITY | UACC] NOT ALTERED

Explanation: An error occurred during ALTUSER command processing.

System action: The AUTHORITY or UACC fields are not altered.

ICH21012I AUTHORIZED TO ISSUE ONLY UAUDIT/NOUAUDIT FOR userid; REMAINING OPERANDS IGNORED

Explanation: You specified operands in addition to UAUDIT or NOUAUDIT, but for the indicated user ID, you are only authorized to specify the UAUDIT or NOUAUDIT operands.

System action: All operands other than UAUDIT or NOUAUDIT are ignored.

User response: See your RACF security administrator.

ICH21013A ENTER OPERATOR IDENTIFICATION CARD

Explanation: You have specified the OIDCARD operand. This message is requesting that you enter the operator identification card for the user being altered so that the information above it can be put into the profile of the user.

System action: Command processing waits for you to enter the operator identification card.

ICH21014I COMMAND ENDED DUE TO ERROR TERMINAL TYPE NOT SUPPORTED

Explanation: You specified the OIDCARD operand, but when the operator identification card was entered, it cannot be verified because it was entered on a terminal that is not supported.

System action: The ALTUSER command stops processing.

ICH21015I CLASS class-name AND REMAINING CLASSES NOT ALTERED FOR CLAUTH/NOCLAUTH

Explanation: The indicated class and all remaining class names in the CLAUTH/NOCLAUTH list were not added to or deleted from the list of authorized classes in the user profile because an error occurred in the RACF manager.

System action: A RACF-manager error message precedes this message and explains the error. Other operands on the command have been processed.

ICH21016I PASSWORD CHANGE FOR 'id' SUPPRESSED BY INSTALLATION PASSWORD EXIT

Explanation: The proposed password, as specified in the PASSWORD operand on the ALTUSER command, does not obey the syntax rules of the installation. (These rules were specified by the PASSWORD keyword, RULEn option, on the SETROPTS command.)

System action: Command processing stops.

User response: See your RACF security administrator for the rules regarding new passwords.

ICH21017I NOT AUTHORIZED TO SPECIFY MODEL/NOMODEL, OPERAND IGNORED

Explanation: You do not have sufficient authority to specify MODEL or NOMODEL on the ALTUSER command.

System action: RACF ignores the operand and continues command processing with the next operand.

User response: See your RACF security administrator.

ICH21018I WARNING, UNABLE TO LOCATE THE MODEL PROFILE FOR dname

Explanation: You have specified a model profile data set name that cannot be found on the RACF database. For modeling to be effective for this data set name, a data set profile must first be created.

System action: RACF adds the data set name you specified to the user profile in anticipation that profile information for this name is completed (by using the
ADDSD command) at a later time. RACF continues to process the ALTUSER command.

ICH21019I  'RESUME' IGNORED. userid NOT CURRENTLY REVOKED

Explanation: The indicated user ID is not currently revoked.

System action: RACF ignores the specification of a future date with the RESUME operand.

ICH21020I  category ALREADY DEFINED TO profile-name

Explanation: The specified category has already been defined in this profile.

System action: RACF ignores the category and continues command processing with the next operand.

ICH21021I  category NOT DEFINED TO profile-name

Explanation: Because the specified category has not been defined in this profile, RACF cannot delete it.

System action: RACF ignores the category and continues command processing with the next operand.

ICH21022I  'REVOKE' IGNORED. userid IS CURRENTLY REVOKED

Explanation: REVOKE was specified with a date, but the user is already revoked.

System action: RACF ignores REVOKE processing and continues command processing with the next operand.

ICH21023I  COMMAND PROCESSING TERMINATED. NO [SECLEVELS | CATEGORIES] FOUND

Explanation: RACF cannot validate the name you specified on the SECLEVEL or ADDCATEGORY operand. This happened for one of two reasons:
- There is no SECLEVEL or CATEGORY profile.
- A profile is defined, but it does not contain any members.

System action: Command processing stops.

ICH21026I  NOT AUTHORIZED TO SPECIFIED FIELD(S) IN segment-name SEGMENT

Explanation: You are not authorized to update the fields specified on the ALTUSER command in segment segment-name.

System action: Command processing stops with no update to the RACF database.

User response: See your RACF security administrator for authority to the DFP segment of this group profile.

RACF Security Administrator Response: You can use field-level access checking to allow this user to add DFP segment information. For a description of field-level access checking, see z/OS Security Server RACF Security Administrator's Guide.

ICH21027I  COMMAND PROCESSING COMPLETED BUT UNABLE TO UPDATE 'SYS1.BRODCAST'.

Explanation: The command you issued has been completed; however, your attempt to change the TSO/E data set SYS1.BRODCAST has failed.

ICH21028I  segment-name OPERAND NOT PROCESSED

Explanation: You are not authorized to change the specified segment.

System action: None of the operands for this segment are processed.

User response: See your RACF security administrator for authority to this segment.

ICH21029I  CONFLICT BETWEEN SIZE AND MAXSIZE. OPERAND IS IGNORED.

Explanation: The SIZE and MAXSIZE operands differ.

System action: Both operands are ignored.

ICH21030I  SIZE SPECIFIED GREATER THAN MAXSIZE. SIZE ADJUSTED EQUAL TO MAXSIZE.

Explanation: The specified size is greater than the maximum allowable size, as specified on the MAXSIZE operand.

System action: RACF adjusts the size to equal the MAXSIZE operand.

User response: You can adjust the SIZE and MAXSIZE operands by using the ALTUSER command.

ICH21031I  ALTUSER failed. NOSECLABEL is not allowed under the current RACF options.

Explanation: NOSECLABEL operand was specified on the ALTUSER command, and SETROPTS MLACTIVE is on.

System action: Command processing stops.

User response: Correct the command.
ICH21032I  ALTUSER failed. SECLABEL seclabel-name is not currently defined to RACF.

Explanation: There is no profile in class SECLABEL whose name is the security label indicated in the message.
System action: Command processing stops.
User response: Check the spelling of the value specified on the SECLABEL operand. If it is correct, define a profile of that name in the SECLABEL class. If you cannot define such a profile, report the exact text of this message to your RACF security administrator.

ICH21033I  ALTUSER failed. User is not connected to group group-name

Explanation: The indicated group name was specified in the DFLTGRP operand, but the user is not yet connected to the group.
System action: The command continues, but the DFLTGRP is not updated in the user profile.
User response: Correct the DFLTGRP operand, or use the CONNECT operand to connect the user to the specified group name and issue the command again.

ICH21034I  PASSWORD CHANGE REJECTED BY INSTALLATION SYNTAX RULES

Explanation: You specified a potential password that does not adhere to the syntax rules that are in effect for your installation.
System action: RACF ignores the operand and continues command processing with the next operand.
User response: See your RACF security administrator for the syntax rules for passwords.

ICH21035I  User username is assigned an OMVS UID, but default group grpname does not have a GID. Processing continues.

Explanation: This is a warning message that gets issued if a user with an OMVS UID gets changed and has a default group that does not have a GID.
User response: This usage violates documented rules. Either the default group should be assigned a GID, or the UID should be removed from the user profile.
RACF Security Administrator Response: Follow documented guidelines to assure that default groups for (OMVS users with UIDs) have GIDs assigned.

ICH21036I  PASSWORD CHANGE REJECTED DUE TO INSTALLATION MINIMUM CHANGE INTERVAL

Explanation: The ALTUSER command has detected that an insufficient number of days has passed since your last password change.
System action: RACF ignores the operand and continues command processing with the next operand.
User response: Contact your security administrator to determine your installation's minimum password change interval, and to reset your password if it has been compromised.

ICH21037I  PASS PHRASE CHANGE REJECTED DUE TO INSTALLATION MINIMUM CHANGE INTERVAL

Explanation: The ALTUSER command has detected that an insufficient number of days has passed since your last password phrase change.
System action: RACF ignores the operand and continues command processing with the next operand.
User response: Contact your security administrator to determine your installation's minimum password change interval because it also applies to password phrases, and reset your password phrase if it has been compromised.

ICH21038I  PASS PHRASE CHANGE REJECTED BY INSTALLATION PASS PHRASE EXIT

Explanation: The proposed password phrase, as specified in the PHRASE operand on the ALTUSER command, has been rejected by the installation password phrase exit, ICHPWX11.
System action: RACF ignores the operand and continues command processing with the next operand.
User response: See your RACF security administrator for the rules regarding new password phrases.

ICH21039I  NEW PASS PHRASE REJECTED BY RACF RULES

Explanation: You specified a potential password phrase that does not adhere to the following syntax rules:
• The user ID is not part of the password phrase.
• At least 2 alphabetics are specified (A - Z, a - z).
• At least 2 non-alphabetics are specified (numerics, punctuation, special characters).
• No more than 2 consecutive characters are identical.
System action: RACF ignores the operand and continues command processing with the next operand.
User response: Try again with a different password phrase.

ICH21040I  PHRASE OPERAND IGNORED

Explanation: You specified the PHRASE operand but the user currently has no password assigned. Users cannot have only a password phrase; they must also have a password.

System action: RACF ignores the NOPASSWORD operand.

ICH21041I  NOPASSWORD OPERAND IGNORED

Explanation: You specified the NOPASSWORD operand but either the user currently has a password phrase assigned, or you also specified the PHRASE operand. A user must have a password if a password phrase is assigned.

System action: RACF ignores the NOPASSWORD operand.
**ALTDSD command messages**

ICH22001I profile-name NOT DEFINED TO RACF

**Explanation:** The profile indicated in the message is not defined to RACF and cannot be altered.

**System action:** Processing continues with the next profile name.

**Note:** If you enter the ALTDSD command for a fully qualified generic profile (one whose name has no generic characters), but you do not specify the GENERIC operand, RACF issues this message. This occurs because, without the GENERIC operand, RACF looks for a discrete profile of that name. For example, if there is a fully qualified generic profile named ABC.DATA, and you enter the following command:

```
ALTDSD 'ABC.DATA'
```

RACF looks for a discrete profile named ABC.DATA and, if there is none, issues this message (ICH22001I ABC.DATA NOT DEFINED TO RACF). To identify for RACF the generic profile, specify the GENERIC operand as follows:

```
ALTDSD 'ABC.DATA' GENERIC
```

ICH22002I NOT AUTHORIZED TO SPECIFY OWNER

**Explanation:** You do not have sufficient authority to specify the OWNER operand.

**System action:** The owner field is not changed. Processing continues with the next operand of the ALTDSD command.

**User response:** See your RACF security administrator.

ICH22003I NOT AUTHORIZED TO ISSUE ALTDSD

**Explanation:** One of the following conditions is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

**System action:** Command processing stops.

**User response:** If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

**RACF Security Administrator Response:** If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or the authority required to issue the indicated command, see [z/OS Security Server RACF Command Language Reference](https://www.ibm.com).
**System action:** Processing for the ADDVOL or ALTVOL operand stops.

**ICH22010I** VOLUME SPECIFIED DOES NOT EXIST IN DATASET PROFILE

**Explanation:** The DELVOL or ALTVOL operand was specified that requests a volume to be deleted from the data set profile but the volume does not exist in the profile.

**System action:** Processing for the DELVOL or ALTVOL operand stops.

**ICH22011I** VOLUME SPECIFIED IS LAST VOLUME IN DATASET PROFILE. NO CHANGE MADE

**Explanation:** The DELVOL operand was specified which requested that the last volume be deleted from the data set profile. This is not a valid request for the ALTDSD command.

**System action:** Processing for the DELVOL operand stops.

**ICH22012I** NOT AUTHORIZED TO SPECIFY NOSET/ALTVOL

**Explanation:** You do not have sufficient authority to specify the NOSET or ALTVOL operand.

**System action:** The NOSET, ADDVOL, ALTVOL, and DELVOL operands are ignored.

**User response:** See your RACF security administrator.

**ICH22013I** ADDVOL/DELVOL NOT PROCESSED

**Explanation:** While adding or deleting a volume, the command processor cannot establish the required ESTAE recovery environment. Other operands have already been processed.

**User response:** Report this message to your system programmer. Include the following information:
- The message ID
- The exact wording of the command you entered
- The date and time you entered the command.

**System programmer response:** Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

**ICH22014I** NOT AUTHORIZED TO SPECIFY GLOBALAUDIT FOR profile-name; OPERAND IGNORED

**Explanation:** You do not have sufficient authority to specify the GLOBALAUDIT operand for the indicated profile name.

**System action:** RACF ignores the operand for the indicated profile name.

**User response:** See your RACF security administrator.

**ICH22015I** AUTHORIZED TO ISSUE ONLY GLOBALAUDIT FOR profile-name; REMAINING OPERANDS IGNORED

**Explanation:** You do not have sufficient authority to specify any operand except GLOBALAUDIT for the indicated profile name.

**System action:** RACF ignores all other operands for the indicated profile name.

**User response:** See your RACF security administrator.

**ICH22016I** VOLUME SPECIFIED ALREADY EXISTS IN ANOTHER PROFILE FOR SAME DATA SET NAME

**Explanation:** An ADDVOL or ALTVOL request was specified, but the volume serial number to be added to the data set profile specified is already defined in another data set profile of the same name.

**System action:** The volume serial number is not added.

**ICH22017I** ALTVOL PROCESSING ENDED DUE TO ERROR

**Explanation:** While processing the ALTVOL operand, the command processor encountered an error that caused processing to stop. Other operands have already been processed.

**ICH22018I** INSTALLATION EXIT FAILED ALTER REQUEST FOR profile-name

**Explanation:** The command preprocessing exit routine ICHCNX00 issued a return code of 4, indicating that RACF should fail the ALTDS D request for the profile name indicated in the message.

**System action:** Command processing stops.

**User response:** Report this message to your system programmer.

**ICH22020I** GENERIC INVALID, GENERIC COMMAND PROCESSING NOT ACTIVE

**Explanation:** Because the generic command processing facility is inactive, the GENERIC operand is not valid.

**System action:** Command processing stops.
**ICH22021I** category ALREADY DEFINED TO profile-name.

**Explanation:** The specified category has already been defined in this profile.

**System action:** RACF ignores the category. Command processing continues with the next operand.

**ICH22022I** category NOT DEFINED TO profile-name.

**Explanation:** The specified category has not been defined in this profile; therefore, deletion is impossible.

**System action:** RACF ignores the category. Command processing continues with the next operand.

**ICH22023I** 'NOTIFY IGNORED' SPECIFIED USER IS NOT DEFINED TO RACF

**Explanation:** The user ID specified for the NOTIFY operand is not a RACF-defined user ID.

**System action:** Command processing continues with the next operand.

**ICH22024I** NOT AUTHORIZED TO USE VOLUME volume

**Explanation:** You do not have allocation authority to the volume specified.

**System action:** Command processing stops.

**User response:** See your RACF security administrator.

**ICH22025I** UNABLE TO LOCATE TAPE VOLUME ENTRY FOR TAPE DATA SET dsname

**Explanation:** A TVTOC entry cannot be located after a discrete profile for the tape data set indicated by dsname was found. RACF searched for a TVTOC entry in one of the following places:
- The TVTOC of the volume specified in the ADDVOL or DELVOL operand of the ALTDSD command
- The TVTOC of the volume specified in the data set profile, if ADDVOL and DELVOL were not specified on the ALTDSD command and this is a tape data set.

**System action:** Command processing continues with the next data set.

**User response:** Do one of the following tasks:
- If ADDVOL or DELVOL was specified on the ALTDSD command, check the spelling of the volume specified on the ADDVOL or DELVOL operands. If the spelling is correct, check that the volume specified actually contains part of the data set specified.
- If ADDVOL and DELVOL were not specified on the ALTDSD command, do the following tasks:
  1. Use the LISTDSD command to display profile dsname. In the LISTDSD output, check the VOLUME ON WHICH DATASET RESIDES and UNIT fields for a possible error.
  2. If no error is apparent in the LISTDSD output, use the RLIST command to display the profile named in the VOLUME ON WHICH DATASET RESIDES field. Check the output of the RLIST command for a possible error.

**ICH22026I** UNABLE TO LOCATE TAPE VOLUME FOR TAPE DATA SET dsname

**Explanation:** The tape volume profile named in the indicated tape data set profile cannot be located. This error indicates a problem with the RACF database.

**System action:** Command processing continues with the next data set.

**User response:** See your RACF security administrator.

**ICH22027I** ALTVOL OPERAND INCONSISTENT WITH TAPE DS PROFILE FOR DATA SET profile-name.

**Explanation:** A tape data set profile was found when an ALTVOL request was entered. RACF does not support ALTVOL processing for tape data sets.

**System action:** ALTVOL processing continues with the next profile specified on the ALTDSD command.

**ICH22028I** TAPE DATA SET SPECIFIED NOT LAST ON VOLUME - ADDVOL/DELVOL IGNORED

**Explanation:** The ADDVOL or DELVOL operand was entered for a tape data set that is not the last one on the tape volume set.

**System action:** RACF ignores the operand. Command processing continues with the next data set name.
ICH22029I  TVTOC UPDATE FAILED. ADDVOL/DELVOL BYPASSED FOR DATA SET PROFILE dsname

Explanation: When ADDVOL or DELVOL operand processing attempted to update the tape data set entry in the TVTOC of the TAPEVOL profile, a RACF-manager error occurred.

System action: RACF does not update the TVTOC. Command processing continues with the next data set name.

ICH22030I  VOLSER LIST INCONSISTENT WITH ADDVOL/DELVOL OPERAND FOR TAPE DS dsname

Explanation: For ADDVOL, the VOLSER specified in the command was found in the tape volume list. For DELVOL, the VOLSER specified in the command was not found in the list.

System action: The ADDVOL/DELVOL operand for this data set is bypassed. Command processing continues with the next data set name.

ICH22031I  COMMAND PROCESSING TERMINATED. NO {SECLEVELS | CATEGORIES} FOUND

Explanation: RACF cannot validate the name you specified on the SECLEVEL or ADDCATEGORY operand. This happened for one of two reasons:

- There is no SECLEVEL or CATEGORY profile.
- A profile is defined, but it does not contain any members.

System action: Command processing stops.

ICH22032I  NOT AUTHORIZED TO DFP SEGMENT FOR DATASET PROFILE profile-name DATASET PROFILE NOT PROCESSED

Explanation: You specified the RESOWNER operand on the ALTDSD command, but you are not authorized to the DFP segment for the specified data set profile.

System action: Command processing stops with no update to the data set profile.

User response: See your RACF security administrator for authority to the DFP segment of this profile.

RACF Security Administrator Response: You can use field-level access checking to allow this user to add a DFP segment profile. For a description of field-level access checking, see z/OS Security Server RACF Security Administrator's Guide.

ICH22033I  DFP OPERAND NOT PROCESSED

Explanation: You are not authorized to alter the RESOWNER field of the specified data set profile.

System action: Command processing stops.

User response: See your RACF security administrator for authority to this segment.

ICH22034I  ALTDSD failed. You are not authorized to specify SECLABEL or NOSECLABEL.

Explanation: The SECLABEL operand was specified on the ALTDSD command and one of the following conditions is true:

- The user did not have the SPECIAL attribute and SETROPTS SECLABELCONTROL was in effect.
- SETROPTS MLSTABLE was in effect, but SETROPTS MLQUIET was not in effect.

System action: Command processing stops.

User response: See your RACF security administrator.

ICH22035I  ALTDSD failed. SECLABEL seclabel-name is not currently defined to RACF.

Explanation: There is no profile in class SECLABEL whose name is the security label indicated in the message.

System action: Command processing stops.

User response: Check the spelling of the value specified on the SECLABEL operand. If it is correct, report the exact text of this message to your RACF security administrator.

ICH22036I  ALTDSD failed. NOSECLABEL is not allowed under the current RACF options.

Explanation: The NOSECLABEL operand was specified on the ALTDSD command. You cannot do this when SETROPTS MLACTIVE is on.

System action: Command processing stops.

User response: Correct the command.

ICH22037I  ALTDSD failed. You are not authorized to specify SECLABEL seclabel-name.

Explanation: To specify the security label indicated in the message, you must have at least READ access authority to the SECLABEL profile indicated in the message.

System action: Command processing stops.

User response: See your RACF security administrator.
### LISTUSER command messages

#### ICH30001I  UNABLE TO LOCATE [USER | GROUP | CONNECT] ENTRY profile-name

**Explanation:** The indicated profile name cannot be found on the RACF database.

**System action:** If a user profile cannot be located, processing continues with the next profile. If a group or connect profile cannot be located, then an inconsistency exists on the RACF database.

**Problem Determination:** The RACF utility programs may be needed to determine the inconsistency. All information that is available is listed.

#### ICH30002I  NOT AUTHORIZED TO LIST userid, *

**Explanation:** You do not have sufficient authority to list the indicated user ID or to specify *.

**System action:** Command processing stops.

**User response:** If you are attempting to list your own user ID, enter the LISTUSER command without operands. Otherwise, see your RACF security administrator.

#### ICH30003I  GROUP group-name USER CONNECTION NOT INDICATED

**Explanation:** The user profile being listed identifies the indicated group as a connected group, but the group profile does not reference the user. An inconsistency exists on the RACF database.

**Problem Determination:** The RACF utility programs may be needed to determine the inconsistency. All information that is available is listed.

#### ICH30010I  NOT AUTHORIZED TO ISSUE LISTUSER

**Explanation:** One of the following conditions is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

**System action:** Command processing stops.

**User response:** If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

**RACF Security Administrator Response:** If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. On adding or altering user profiles or the authority required to issue the indicated command, see z/OS Security Server RACF Command Language Reference.

#### ICH30011I  NO USERS LISTED.

**Explanation:**

- You issued LISTUSER *, but you are not authorized to list any users,
- or
- You issued LISTUSER * segment-name NORACF, and no users with the specified segment were found.

#### ICH30012I  NO USER(S) LISTED. NORACF SPECIFIED AND NO OTHER SEGMENTS REQUESTED.

**Explanation:** RACF cannot list users when NORACF is specified. Listing users for other segments has not been requested.

**System action:** Command processing stops with no output produced.

**User response:** If you specify NORACF, you must specify an operand that requests output, such as DFP, TSO/E, or DSNS.

#### ICH30014I  LISTUSER failed. Parameter list error detected while translating a SECLABEL.

**Explanation:** An internal RACF error has been detected.

**System action:** Command processing stops.

**User response:** Report this message to your system programmer.

**System programmer response:** Report this message to your IBM support center.

#### ICH30015I  This SECLABEL is not currently defined to RACF.

**Explanation:** The security label specified in the user profile does not exist as a profile in the SECLABEL class.

**System action:** Command processing continues without listing the description of the security label.

**User response:** Report this message to your RACF security administrator.
SEARCH command messages

ICH31001I  NOT AUTHORIZED TO ISSUE
  command-name

Explanation: One of the following conditions is true:
  • RACF is inactive.
  • You are not defined to RACF and cannot issue RACF commands.
  • You are not defined to RACF with sufficient authority to issue this command.

System action: Command processing stops.

User response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or the authority required to issue the indicated command, see z/OS Security Server RACF Command Language Reference.

ICH31002I  UNABLE TO OPEN CLIST DATASET, COMMAND TERMINATED

Explanation: SEARCH command processing SEARCH cannot open the specified CLIST data set.

System action: Command processing stops.

ICH31003I  MASK TOO LONG, COMMAND TERMINATED

Explanation: The character string specified on the MASK operand is longer than the maximum allowable length for the profile name in the specified class. For the DATASET class, the maximum length is 44 characters; for the DASDVOL and TAPEVOL classes, the maximum length is 6 characters; and for the TERMINAL class, the maximum length is 8 characters.

System action: Command processing stops.

ICH31004I  LIST AND CLIST OMITTED, COMMAND TERMINATED

Explanation: CLIST must be specified on the SEARCH command when NOLIST is specified.

System action: Command processing stops.

ICH31005I  NO ENTRIES MEET SEARCH CRITERIA

Explanation: One or more of the following conditions occurred:
  • There are no RACF profiles that meet the search criteria.
  • You do not have sufficient authority to list the profiles that match the search criteria.

ICH31006I  CLIST DATA SET ORGANIZATION IS NOT SEQUENTIAL OR PARTITIONED. COMMAND TERMINATED.

Explanation: The CLIST data set for the SEARCH command must have either the physical sequential (PS) organization or the partitioned organization (PO). The CLIST data set found does not have one of these organizations.

User response: See your system programmer.

System programmer response: Make sure the CLIST data set, userid.EXEC.RACF.CLIST, is either a partitioned data set or a sequential data set.

System action: Command processing stops.

ICH31007I  COMMAND ENDED DUE TO ERROR

Explanation: A RACF manager error occurred. This message is accompanied by a message explaining the error.

ICH31008I  CATEGORY category-name IGNORED

Explanation: The user does not have sufficient authority to list the entries in the RACF data set for the security category name specified on the command, or the security category name does not exist.

User response: See your RACF security administrator.

ICH31009I  FILTER STRING LONGER THAN PROFILE NAMES

Explanation: A filter string was specified longer than the maximum allowable for a profile name in that class.

System action: Command processing stops.

ICH31010I  FILTER AND MASK BOTH SPECIFIED

Explanation: The FILTER operand is an alternative to the MASK operand; they are mutually exclusive.

System action: Command processing stops.

ICH31011I  BLANK FOUND IN FILTER STRING

Explanation: The filter string cannot contain blanks.

System action: Command processing stops.
User response: Check the spelling of the value specified on the SECLABEL operand. If it is correct, report the exact text of this message to your RACF security administrator.

ICH31028I The [UID|GID] keyword requires application identity mapping to be implemented.

Explanation: The UID or GID keyword has been specified on the SEARCH command, but the RACF database has not been converted to the use of application identity mapping. Application identity mapping must be enabled in order for SEARCH to be able to map UIDs and GIDs to USER and GROUP profiles. Use of the UNIXMAP class is not sufficient. The RACF database must be at least at stage 2 of application identity mapping.

System action: Command processing stops.

System programmer response: Use the IRRIRA00 utility to convert the RACF database to at least stage 2 of application identity mapping. See the z/OS Security Server RACF System Programmer’s Guide for information about the IRRIRA00 utility. Once this is complete, the user may reissue the command.

User response: Contact your system programmer.
LISTGRP command messages

ICH32002I  NOT AUTHORIZED TO LIST BASE INFORMATION FOR GROUP
          group-name

Explanation: You do not have sufficient authority to list the group profile indicated in the message.

System action: Command processing continues with the next group specified.

User response: See your RACF security administrator.

ICH32004I  NOT AUTHORIZED TO ISSUE LISTGRP

Explanation: One of the following conditions is true:
- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

System action: Command processing stops.

User response: If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

RACF Security Administrator Response: If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or the authority required to issue the indicated command, see z/OS Security Server RACF Command Language Reference.

ICH32005I  NO GROUPS LISTED

Explanation:
- You issued LISTGRP *, but are not authorized to list any groups,
  or
- You issued LISTGRP * segment-name NORACF, and no groups with the specified segment were found.

User response: See your RACF security administrator.

ICH32006I  NOT AUTHORIZED TO DISPLAY DFP SEGMENT IN GROUP PROFILE
          group-name

Explanation: You are not authorized to display a DFP segment.

System action: Command processing stops.

User response: See your RACF security administrator for authority to this segment.

RACF Security Administrator Response: See the command description in z/OS Security Server RACF Command Language Reference for the authority required to list the indicated segment.

ICH32007I  NO SEGMENT REQUESTED

Explanation: You specified NORACF (which requests no display for the RACF segment of a group profile), but you did not specify any other segment (such as DFP).

System action: Command processing continues with no segment displayed.

User response: Either specify another segment to be displayed or omit the NORACF operand. Enter the command again.
LISTDSD command messages

ICH35001I  COMMAND ENDED DUE TO ERROR

**Explanation:** A RACF-manager error occurred. This message is accompanied by a message explaining the error.

ICH35002I  NOT AUTHORIZED TO LIST

**Explanation:** You do not have sufficient authority to the profile indicated in the message and cannot list the profile.

**System action:** Command processing continues with the next profile.

**User response:** See your RACF security administrator.

ICH35003I  NO RACF DESCRIPTION FOUND FOR

**Explanation:** No profile can be found in the RACF database for the data set indicated in the message for one of the following reasons:

- The data set profile does not exist.
- The data set profile requested is a fully qualified generic, and the GENERIC operand was not specified in the command string.
- The data set profile requested is discrete, the GENERIC operand was specified, and there is no generic profile that closely matches the discrete profile name.

**User response:** If the LISTDSD command was issued without the GENERIC operand, and this data set profile is generic, issue the command again with the GENERIC operand. If the LISTDSD command was issued with the GENERIC operand, and this data set profile is discrete, issue the command again without the GENERIC operand.

ICH35004I  NOT AUTHORIZED TO ISSUE LISTDSD

**Explanation:** One of the following conditions is true:

- RACF is inactive.
- You are not defined to RACF and cannot issue RACF commands.
- You are not defined to RACF with sufficient authority to issue this command.

**System action:** Command processing stops.

**User response:** If RACF is inactive, try to log on when RACF is active. Otherwise, see your RACF security administrator.

**RACF Security Administrator Response:** If the user is not defined to RACF, consider adding the person to the RACF database. If the user does not have sufficient authority, consider granting additional authority. For more information about adding or altering user profiles or the authority required to issue the indicated command, see [z/OS Security Server RACF Command Language Reference](https://www.ibm.com/support/docview.ws/docview/34854).
System action: Command processing continues with no segment displayed.

User response: Either specify other output to be listed (such as the DFP or DSNS operand) or omit the NORACF operand. Enter the command again.

ICH35011I LISTDSD failed. Error encountered during catalog processing.

Explanation: LISTDSD DSNS was issued, but there are no cataloged data sets that are protected by the specified profile.

System action: The command executes but no data set names are displayed.

ICH35012I LISTDSD cannot obtain this data in an MVS/370 environment.

Explanation: LISTDSD DSNS was issued from an MVS/370 environment. The DSNS operand is not supported in an MVS/370 environment.

System action: The command executes but no data set names are displayed.
Chapter 3. Miscellaneous RACF ICH messages

This section lists the messages issued by:
- RACF command processors, when the messages reflect errors in the RACF manager
- RACF report writer
- Data security monitor

RACF routes these messages to the user.

The format of these messages is:
ICHxxnnnt text

where:
ICH identifies the message as a RACF message.
xx identifies the function issuing the message.
nnn is the message serial number.
t is the type code (I = information, or A = action).
text is the text of the message.

The values for the xx field that identifies the function issuing the message are:

<table>
<thead>
<tr>
<th>xx</th>
<th>Function/Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>51</td>
<td>RACF manager (see “Note”)</td>
</tr>
<tr>
<td>64</td>
<td>RACF report writer (RACFRW)</td>
</tr>
<tr>
<td>66</td>
<td>Data security monitor (DSMON)</td>
</tr>
<tr>
<td>70</td>
<td>Miscellaneous</td>
</tr>
</tbody>
</table>

**Note:** These common error messages are issued by the various RACF command processors based on return codes from the RACF manager.

### RACF manager error messages

**ICH51001I** SVC 132 UNABLE TO INVOKE PROCESSING ROUTINE

**Explanation:** RACF was unable to invoke the appropriate processing routine (RACF manager, RACROUTE REQUEST=LIST) because of one of the following errors, whose code is returned in register 0:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Unable to establish ESTAE environment.</td>
</tr>
<tr>
<td>1</td>
<td>The function code (third byte of parameter list) does not represent a valid function.</td>
</tr>
</tbody>
</table>

**ICH51002I** NAME TO BE ADDED TO RACF DATA SET ALREADY EXISTS

**Explanation:** The user or group name that was requested to be added to the RACF database already exists on the RACF database; for example, if you attempted to add user X, and group X already exists.

**ICH51003I** NAME NOT FOUND IN RACF DATA SET

**Explanation:** A profile requested by the command does not exist on the RACF database. If the command does not issue a message giving the profile name, the RACF list commands (LISTDSD, LISTGRP, and LISTUSER) can be used to determine inconsistencies in profiles associated with the command.

**ICH51004I** PARAMETER LIST ERROR DETECTED

© Copyright IBM Corp. 1994, 2012
BY RACF MANAGER

Explanation: The RACF manager has detected one of the following errors:
- Input parameter list error. The following codes are returned in register 0:
  
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Entry name (profile name) incorrect</td>
</tr>
<tr>
<td>2</td>
<td>Action specified for delete</td>
</tr>
<tr>
<td>3</td>
<td>Incorrect field name</td>
</tr>
<tr>
<td>4</td>
<td>Test specified for rename request</td>
</tr>
<tr>
<td>7</td>
<td>Entry type (profile type) incorrect.</td>
</tr>
</tbody>
</table>
- User work area not large enough to hold all the data.
- User work area smaller than minimum allowable size.

ICH51005I ATTEMPT TO DELETE RESTRICTED NAME DENIED BY RACF MANAGER

Explanation: An attempt was made to delete a restricted name.

ICH51006I ALTER IN PLACE REQUEST REJECTED BY RACF MANAGER

Explanation: The requested ALTERI operation is invalid.

ICH51007I RACF DATABASE CANNOT BE ALTERED.

Explanation: The RACF database cannot be altered for one or more of the following reasons:
- The database has been locked by a RACF utility.
- The system that attempted to alter the database is currently in read-only mode (in a RACF sysplex data sharing environment).

ICH51008I DUPLICATE DATASET NAME FOUND BUT VOLUME NOT SPECIFIED

Explanation: In processing a data set request, the RACF manager found duplicate data set profiles in the RACF database and did not process the request because the VOLUME operand was not specified on the request.

ICH51009I VOLUME NOT FOUND

Explanation: In processing a data set request, the RACF manager searched all the data set profiles that have the name specified in the command. However, the RACF manager cannot find the volume serial number that you specified in any of those profiles.

ICH51010I RACF DATASET ACCESS DENIED–RACF IS NOT ACTIVE OR THE RACF DATASET CONTAINING THE REQUESTED PROFILE NOT ACTIVE

Explanation: The RACF manager cannot complete the requested operation because RACF is currently not active.

ICH51011I RACF MANAGER PROCESSING ENDED DUE TO ERROR. RETURN CODE = return-code

Explanation: The RACF manager cannot complete the requested operation because of a system error, command processor error, or a problem with the RACF database. The return code, which is displayed in decimal format, is a RACF manager return code that is not recognized by the command processor that invoked the RACF manager.

Problem Determination: For certain errors in the RACF database, the RACF manager may issue message IRR411I preceding this message. See this message for information about how to resolve the problem.

Note: If the user is not receiving write-to-programmer messages, message IRR411I cannot be received. To receive this message, issue the TSO/E command PROFILE WTPMSG MSGID and rerun the RACF command or utility.

Check the list of RACF-manager return codes in "RACF manager return codes" on page 405. If the return code is listed, the explanation should help you investigate the problem. If the return code is not listed or relates to a problem with RACF (as opposed to a problem you can fix in the RACF database), report the complete text of this message to your IBM support center.

For certain return codes, this message might be issued because there is a bad profile in the RACF database. To find the bad profile, enter the SEARCH command. With a bad profile in the database, this command is likely to fail also. The profile after the last one listed is probably the bad profile. Because this command might take a long time to run and might produce many lines of output, you may want to execute the command in batch.

ICH51012I RACF AUTHORITY DENIED BY FIELD LEVEL ACCESS CHECKING

Explanation: You do not have sufficient authority for access at the field level. The RACF database is not updated.

User response: See your RACF security administrator.
ICH51013I PROFILE ADDED OR ALTERED BUT NO ROOM TO MAKE ALIAS INDEX ENTRY.

Explanation: A user ID was added or altered in a way that specified a UID (such as UID 0), which already has a large number of user IDs that map to it. See [z/OS Security Server RACF System Programmer's Guide](https://publib.boulder.ibm.com/infocenter/prodguid/v5r4/index.jsp?topic=%2Fcom.ibm.racf.doc%2Frsracs000.htm) for more information about the maximum number of user IDs that can map to a single UID.

System action: The changes specified were made to the user profile that goes with the user ID, but no Alias Index entry was updated.

User response: Report this message to your system programmer.

System programmer response: Take action to reduce the number of user IDs that map to the same UID, which is specified on the command that generated this message.

In the mean time, the system is fine and run-wise. The profile has a UID of 0 with no alias index entry (UID 0 is used in this paragraph, although the same can apply to any UID to which a large number of user IDs map). At runtime, only the first profile in the list gets returned when you look up UID=0, which should have the right authorities. What is lost is some of the capability to look up all the user IDs that map to UID 0. Search commands SRCLASS(USER) UID(0) will not return user IDs that do not have alias entries. Likewise, IRRUT200 will miss these entries in the Alias Index part of the output, where base profiles are listed. To find all the users with UID=0 in their profile, it is necessary to run dbunload and use DB2® to query which profiles have UID=0.
## RACF report writer (RACFRW) messages

### ICH64001I  SUBCOMMAND subcommand-name NOT FOUND; ANY SUBCOMMAND ENTERED AFTER subcommand-name MUST BE REENTERED

**Explanation:** The RACF report writer does not support the subcommand name entered.

**System action:** The RACF report writer ignores this subcommand and all subsequent RACF report writer subcommands. The RACF report writer prompts the user to enter another subcommand.

**User response:** The user must enter another subcommand. For more information, see the [z/OS Security Server RACF Auditor’s Guide](https://www.ibm.com/support/docview/mobile/9172).

### ICH64002I  TOO MANY SUBCOMMANDS; IMAGES LOST ON OUTPUT LISTING

**Explanation:** The user has entered more than the maximum number (100) of subcommands that the RACF report writer can reproduce on the output listing.

**System action:** Although all the subcommands are processed, the list of subcommands appearing on the output listing is incomplete. The RACF report writer prompts the user to enter another subcommand.

**User response:** The user must enter another subcommand. For more information, see [z/OS Security Server RACF Auditor’s Guide](https://www.ibm.com/support/docview/mobile/9172).

### ICH64003I  report-name REPORT COMPLETE

**Explanation:** The named report has been completed successfully.

**System action:** The RACF report writer continues with the next report or, if all reports have been processed, ends normally.

### ICH64004I  operand DOES NOT APPLY TO STATUS RECORDS; OPERAND IGNORED

**Explanation:** On the SELECT subcommand, the user has specified the named operand along with the STATUS operand.

**System action:** Because the named operand has no meaning for status records, the RACF report writer ignores it. The RACF report writer prompts the user to enter another subcommand.

**User response:** The user must enter another subcommand. For more information, see [z/OS Security Server RACF Auditor’s Guide](https://www.ibm.com/support/docview/mobile/9172).

### ICH64005I  LIMIT OF 50 SELECT AND EVENT SUBCOMMANDS HAS BEEN EXCEEDED; subcommand-name IGNORED

**Explanation:** The user has entered more than the maximum number (50) of SELECT and EVENT subcommands.

**System action:** The RACF report writer ignores the subcommand. The RACF report writer prompts the user to enter a subcommand other than SELECT or EVENT.

**User response:** The user must enter another subcommand. For more information, see [z/OS Security Server RACF Auditor’s Guide](https://www.ibm.com/support/docview/mobile/9172).

### ICH64006I  OPERAND DOES NOT APPLY TO event-name EVENT; OPERAND IGNORED

**Explanation:** On the EVENT subcommand, the user specified an operand that is not valid for the named event.

**System action:** The RACF report writer ignores the operand. The RACF report writer prompts the user to enter another subcommand.

**User response:** The user must enter another subcommand. For more information, see [z/OS Security Server RACF Auditor’s Guide](https://www.ibm.com/support/docview/mobile/9172).

### ICH64007I  THERE IS NO PRECEDING SELECT SUBCOMMAND FOR THIS EVENT SUBCOMMAND; EVENT IGNORED

**Explanation:** The user has entered an EVENT subcommand without first having entered any SELECT subcommands.

**System action:** The RACF report writer ignores the EVENT subcommand. The RACF report writer prompts the user to enter another subcommand.

**User response:** The user must enter another subcommand. For more information, see [z/OS Security Server RACF Auditor’s Guide](https://www.ibm.com/support/docview/mobile/9172).

### ICH64008I  INVALID SUBCOMMAND

**Explanation:** The user has entered a subcommand that violates the syntax rules for subcommand names.

**System action:** The RACF report writer ignores the subcommand. The RACF report writer prompts the user to enter another subcommand.

**User response:** The user must enter another subcommand. For more information, see [z/OS Security Server RACF Auditor’s Guide](https://www.ibm.com/support/docview/mobile/9172).
ICH64009I NOUSER/NOJOB COMBINATION INVALID; BOTH OPERANDS IGNORED

Explanation: On the SELECT subcommand, the user has specified both the NOUSER and the NOJOB operands.

System action: The RACF report writer ignores both operands and uses the defaults (USER and JOB) to select all user IDs and job names.

User response: Enter next subcommand.

ICH64301I RACFRW ENDED DUE TO PUTGET ERROR + PUTGET RETURN CODE return-code

Explanation: While the RACF report writer was prompting the user to enter a subcommand, an error occurred in the PUTGET TSO/E service routine.

System action: The RACF report writer stops.

User response: See your system programmer.

System programmer response: For an explanation of the TSO/E service routines return codes, see z/OS TSO/E Programming Services. For the order number of the documentation you need, see z/OS TSO/E General Information.

ICH64302I RACFRW ENDED DUE TO IKJSCAN ERROR + IKJSCAN RETURN CODE return-code

Explanation: An error occurred in the IKJSCAN TSO/E service routine while it was checking the syntax of a RACFRW subcommand.

System action: The RACF report writer stops.

User response: See your system programmer.

System programmer response: For an explanation of the TSO/E service routines return codes, see z/OS TSO/E Programming Services. For the order number of the documentation you need, see z/OS TSO/E General Information.

ICH64303I FILE ddbname COULD NOT BE OPENED

Explanation: The RACF report writer cannot open the file identified by ddbname.

System action: The RACF report writer stops.

User response: Ensure that the DD statement exists or that the data set has been preallocated.

ICH64304I SORT ERROR RETURN CODE 'return-code' OCCURRED WHILE PRODUCING 'report-name' REPORT; COMMAND TERMINATED

Explanation: The sort function invoked by RACF (DFSORT) encountered an error while sorting the records for the named report.

System action: The RACF report writer stops.

User response: See your system programmer.

System programmer response: Check for an error in module ICHRSMFI, which is an installation-replaceable module used by the RACF report writer. For an explanation of the sort return codes, see z/OS DFSORT Messages, Codes and Diagnosis Guide.

ICH64305I NO INPUT DATASET ALLOCATED; COMMAND TERMINATED

Explanation: The user did not preallocate the RSMFIN file or did not specify the DATASET operand on the RACFRW command.

System action: The RACF report writer stops.

User response: Preallocate the file RSMFIN or specify the DATASET operand on the RACFRW command. For more information, see z/OS Security Server RACF Auditor’s Guide.
Data security monitor (DSMON) messages

ICH66001I  ICHDSM00 STARTED ON mm/dd/yy AT hh:mm:ss
Explanation: Data security monitor execution began at this date and time.

ICH66021I  FUNCTION name ENDED SUCCESSFULLY
Explanation: The data security monitor performed the specified test function.
System action: Processing continues with the next function.

Note: For an explanation of the test functions that the data security monitor performs, see z/OS Security Server RACF Auditor's Guide.

ICH66003I  ICHDSM00 ENDED ON mm/dd/yy AT hh:mm:ss - RETURN CODE = nn
Explanation: Data security monitor execution stops at this date and time with the specified return code. The return codes that can appear in this message are:

Code  Description
0     The data security monitor completed execution successfully.
16    The execution of one or more test functions was unsuccessful.
20    An attempt to open the data set specified in message ICH66101I failed.

ICH66004I  USER NOT AUTHORIZED TO EXECUTE THE DATA SECURITY MONITOR - RETURN CODE = 16
Explanation: DSMON is not a controlled program, but you cannot execute the DSMON program because you do not have the system AUDITOR attribute.
System action: The program ends with return code 16 and produces no reports.

Note: Because the SYSPRINT data set is not opened unless the user is authorized to execute the data security monitor, the data security monitor issues this message to the programmer's console with a write-to-operator instruction (routing code 11) and to the system security console (routing code 9).
User response: See your RACF security administrator.

ICH66009I  ---START OF INPUT LISTING---
Explanation: The data security monitor has started to read the input control statements from the SYSIN data set. A listing of each control statement follows this message.

ICH66010I  ---END OF INPUT LISTING---
Explanation: The data security monitor has finished reading the input control statements from the SYSIN data set.

ICH66011I  ABOVE CONTROL CARD IGNORED. UNKNOWN TYPE
Explanation: The control statement that precedes the message did not have a valid control statement identifier (FUNCTION, USEROPT, or LINECOUNT) and was not a continuation of the prior statement.
System action: Processing continues with the next control statement.

ICH66012I  ERROR IN ABOVE CONTROL CARD. xxxxxxx IS AN UNKNOWN FUNCTION TYPE AND IS IGNORED
Explanation: The FUNCTION statement that precedes the message includes an invalid function name.
System action: Processing continues with the next control statement.

ICH66013I  ABOVE CONTROL CARD IGNORED. xxxxxxx IS AN UNKNOWN USEROPT TYPE
Explanation: The USEROPT statement that precedes the message includes an invalid function name.
System action: Processing continues with the next control statement.

ICH66014I  ABOVE CONTROL CARD IGNORED. INCORRECT LINECOUNT VALUE
Explanation: The lines per page indicated by the LINECOUNT statement was too great, too small, or non-numeric.
System action: Processing continues with the next control statement.

ICH66015I  EXTRANEOUS INFORMATION IGNORED IN ABOVE CONTROL CARD
Explanation: The LINECOUNT statement contained extra information after the lines per page information.
System action: Processing continues with the next control statement.
ICH66016I  NO xxxxx FUNCTION CARD FOUND.
ANY RELATED USEROPT STATEMENTS WILL BE IGNORED

Explanation:  DSMON found a USEROPT statement for function xxxxx, but there is no matching FUNCTION statement.

System action:  Processing continues with the next control statement.

ICH66017I  ABOVE CONTROL CARD IGNORED.
NO FUNCTION SPECIFIED

Explanation:  DSMON found a function card with no functions specified.

System action:  Processing continues with the next control statement.

ICH66018I  ABOVE CONTROL CARD IGNORED.
INCOMPLETE SPECIFICATION

Explanation:  DSMON found a USEROPT statement with no user value specified. Processing continues with the next control statement.

ICH66019I  ERROR IN ABOVE CONTROL CARD

Explanation:  DSMON found incorrect data on a control statement. Message ICH66020I follows this message.

ICH66020I  FOLLOWING INPUT DATA IGNORED....

Explanation:  The indicated input data is incorrect. DSMON ignores it.

System action:  Processing continues with the next control statement.

ICH66021I  EXPECTED CONTROL CARD CONTINUATION NOT FOUND

Explanation:  The previous input control statement contained a continuation character, indicating that another control statement involving the same statement would follow. DSMON did not find that control statement.

System action:  Processing continues with the next control statement.

ICH66101I  OPEN FAILED FOR DDNAME name

Explanation:  An error occurred during the OPEN issued for the named data set. If the data set that cannot be opened is SYSPRINT, RACF issues this message to the programmer's console with a write-to-operator message (routing code 11).

User response:  See your system programmer.

ICH66102I  FUNCTION name ENDED UNSUCCESSFULLY - ERROR CODE = nnn

Explanation:  The specified test function ended abnormally with the specified error code. This is a right-aligned integer code that can range from 1 to 999.

System action:  Processing continues with the next function.

User response:  See your system programmer.

Problem Determination:  The following table contains a list of the test functions and their associated error codes:

<table>
<thead>
<tr>
<th>Function</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LNKLST</td>
<td>3</td>
<td>An error occurred while attempting to retrieve LNKLST libraries.</td>
</tr>
<tr>
<td>SYSAPF</td>
<td>1</td>
<td>There were no entries in the list of APF libraries.</td>
</tr>
<tr>
<td>SYSLNK</td>
<td>1</td>
<td>An error occurred while attempting to open the SYS1.PARMLIB data set.</td>
</tr>
<tr>
<td>SYSLNK</td>
<td>2</td>
<td>An error occurred while attempting to open SYSUT1.</td>
</tr>
<tr>
<td>SYSPPT</td>
<td>1</td>
<td>RACF cannot locate the program properties table (PPT).</td>
</tr>
<tr>
<td>SYSPPT</td>
<td>2</td>
<td>An error occurred while attempting to load module IEFS060, which contains the program properties table (PPT).</td>
</tr>
<tr>
<td>RACUSR</td>
<td>1</td>
<td>An error occurred while attempting to access a user profile in the RACF database.</td>
</tr>
<tr>
<td>RACUSR</td>
<td>2</td>
<td>An error occurred while attempting to access a group profile in the RACF database.</td>
</tr>
<tr>
<td>RACEXT</td>
<td>1</td>
<td>Either the entry point address of the specified RACF exit did not correspond with the address contained in the RACF communications vector table (RCVT), or an error occurred while attempting to load a RACF exit routine module defined by the installation.</td>
</tr>
<tr>
<td>RACGRP</td>
<td>1</td>
<td>An error occurred while attempting to access a group profile in the RACF database.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In the group tree report, look for &quot;PROFILE NOT FOUND&quot;. If found, then that is the missing profile. You must add it again, with the appropriate OWNER and SUPGROUP.</td>
</tr>
<tr>
<td>RACGAC</td>
<td>1</td>
<td>There are no classes eligible for global access checking.</td>
</tr>
</tbody>
</table>
ICH66103I  RACF IS INACTIVE OR VERSION IS INVALID - ONLY SYSTEM REPORT PRODUCED

Explanation: One of the following conditions occurred: (1) RACF is not installed; (2) RACF is inactive; or (3) the RACF version that is active is before RACF Version 1 Release 6.

System action: The data security monitor produces the system report and ends.

User response: See your system programmer.

ICH66104I  PROGRAM PROPERTIES TABLE NOT FOUND

Explanation: The data security monitor cannot locate the program properties table; therefore, the data security monitor does not produce the program properties table report.

System action: Processing continues with the next function.

User response: See your system programmer.

ICH66105I  RACF MANAGER ERROR - RETURN CODE = return-code

Explanation: The RACF manager encountered an error while attempting to retrieve RACF user attributes, as indicated by the return code in the message.

System action: Processing continues with the next function.

User response: See your system programmer.

Problem Determination: For a description of the return codes see “RACF manager return codes” on page 405.

ICH66106I  ERROR OCCURRED DURING MEMBERLIST RETRIEVAL

Explanation: The data security monitor encountered an error while attempting to retrieve a list of partitioned data set (PDS) members.

System action: Processing continues with the next function.

User response: See your system programmer.

ICH66107I  EXIT name HAS INVALID RCVT ADDRESS

Explanation: The entry point address of the named RACF exit routine does not correspond with the address contained in the RACF communications vector table (RCVT). This difference might indicate a system integrity exposure, or the presence of a vendor product that dynamically installs the exit.

User response: Report the exact text of this message to your system programmer.

System programmer response: If the exit address value in the RCVT is a valid LPA address, you can use services such as IPCS or TSO TEST to locate the entry point address of the named RACF exit routine and the corresponding exit address in the RCVT. Use these services to identify the owner of the routine that the value in the RCVT points to, and then determine if the difference is expected. If the difference is not expected, use a facility such as SLIP to interrupt the routine that is modifying the named RCVT entry, and determine the reason for this difference. For information about exit addresses in the RCVT, see z/OS Security Server RACF Data Areas.

ICH66108I  ERROR OCCURRED WHILE LOADING EXIT name

Explanation: RACF attempted to load the RACF exit routine, but cannot find this installation-defined module. This error message might indicate a system integrity exposure, or the presence of a vendor product that dynamically installs the exit.

User response: Report the exact text of this message to your system programmer.

System programmer response: If the exit address value in the RCVT is a valid LPA address, you can use services such as IPCS or TSO TEST to locate the entry point address of the named RACF exit routine and the corresponding exit address in the RCVT. Use these services to identify the owner of the routine that the value in the RCVT points to, and then determine if the difference is expected. If the difference is not expected, use a facility such as SLIP to interrupt the routine that is modifying the named RCVT entry, and determine the reason for this difference. For information about exit addresses in the RCVT, see z/OS Security Server RACF Data Areas.

ICH66109I  NO PROFILE EXISTS FOR DATA SET name

Explanation: Although the RACF indicator for the specified data set is on, no resource profile or UACC has been defined.

User response: Report the exact text of this message to your system programmer.

ICH66110I  NO ENTRIES IN THE RACF CLASS DESCRIPTOR TABLE

Explanation: No entries were found in the class descriptor table supplied by IBM or the installation class descriptor table.

System action: RACF processing does not occur.
Processing continues with the next function.

User response: Report this message to your RACF security administrator.

**ICH66111I**  RACF GLOBAL ACCESS TABLE NOT FOUND

Explanation: DSMON cannot locate the global access table.

System action: It does not execute function RACGAC, which obtains the entry name and global-access authority level for all classes eligible for global access checking. DSMON continues processing with the next function.

User response: See your system programmer.

**ICH66121I**  An error occurred during retrieval of LNKLST libraries

Explanation: The data security monitor encountered an error while attempting to retrieve a list of LNKLST libraries.

System action: Processing continues with the next function.

User response: Contact your system programmer.

System programmer response: This message indicates a probable RACF or MVS error. Contact the IBM support center for assistance.

**ICH66134I** USER NOT AUTHORIZED TO RECEIVE USRDSN LISTING

Explanation: You do not have the required authority to profile ICHDSM00.SYSCAT in class FACILITY.

System action: DSMON only reports on the master catalog. No report is made on the user catalogs.

User response: See your RACF security administrator.

**ICH66136I** MAXIMUM NUMBER OF PROCESSABLE USRDSNS FOR CURRENT REGION SIZE EXCEEDED

Explanation: DSMON did not execute successfully, because of storage constraints.

System action: The job ends with return code 8.

User response: Notify your system programmer.

**ICH66137I** EITHER INCREASE THE REGION SIZE AS MUCH AS POSSIBLE AND RERUN THE JOB OR RUN A MULTISTEP JOB

Explanation: Not enough storage was available, given the current JCL REGION parameter, for DSMON to process all user data sets as specified.

System action: The job ends with return code 8.

User response: Notify your system programmer.

Programmer response: The job may run successfully if a larger REGION can be specified. If this is impossible, or if the job fails with larger REGIONs, submit a multistep job, breaking up the user data sets into portions as indicated by the messages that follow this one. If possible, isolate the USRDSN USEROPTS into their own steps. If a substantial number of RACGRP USEROPTS are specified in the JCL, isolate these into their own job steps also. Steps in which only USRDSNs or RACGRPS are specified should specify FUNCTION USRDSN or FUNCTION RACGRP to avoid the default (FUNCTION ALL) processing.

Programmer response:Increase the REGION JCL parameter as much as possible and rerun the job. If this fails, try submitting a multistep job with the user options (data sets/groups) distributed among two or more job steps. Watch for ICH66138I or ICH66137I messages and instructions that might accompany the initial multistep jobs submitted.

**ICH66140I** PROGRAM PROPERTIES TABLE SCAN (IEFPSPCN) ERROR

Explanation: An error was returned to the data security monitor (DSMON) from the program properties table scan service (the IEFPPSCN macro).

System action: The job ends with return code 16.

User response: Notify your system programmer.

Programmer response: This failure may be due to a dynamic Program Properties Table update. Rerun DSMON to see if the problem persists.
ICH66141I UNEXPECTED ICHEINTY ERROR, RC = retcode, RSN = rsncode, ENTRY = entry_name [G].

Explanation: This message is issued when processing the RACSPT (started procedure table) report during execution of DSMON (ICHDSM00). An unexpected error occurred from an ICHEINTY macro used to retrieve information for the STDATA segment for a profile in the STARTED class. This message gives the decimal return and reason codes, and the profile name from the RACF database that caused the error, or that was last processed. If the profile name is generic, it is followed by (G).

System action: The RACSPT report consists of two phases when the STARTED class is active. Phase 1 processes the STARTED class and phase 2 processes the started procedures table (ICHRIN03). Phase 1 has ended and processing continues normally with phase 2. Message ICH66102I (with error code 1) is issued to SYSPRINT to record the unsuccessful completion of part of the RACSPT report. At the conclusion of processing, ICHDSM00 ends with a return code of 16.

User response: Show the SYSPRINT and SYSUT2 output of ICHDSM00 to your system programmer.

System programmer response: Use the return and reason code information in z/OS Security Server RACF Macros and Interfaces and the profile name to determine the error condition and fix the error. If necessary, contact the IBM support center.
RACF miscellaneous messages

ICH70001I userid LAST ACCESS AT hh:mm:ss ON day_of_week, month, day, year

Explanation: This message displays the last recorded date and time that user userid accessed the system. Some examples are:

- The last recorded date and time user userid logged on successfully.
- The last recorded date and time user userid submitted a batch job.

When a user logs on for the first time or for the first time after the RESUME date, the date and time are displayed in asterisks. For example, hh:mm:ss is displayed as **:**:**.

Notes:
1. This message does not reflect all accesses done through APPC.
2. This message is suppressed for started procedures because of a time lapse between the time the procedure starts and when its JOBLOG is activated. It is replaced by MVS message IEF695I identifying the started procedure and its associated user and group ID.
3. Applications can be configured to record only the first logon of the day. When a user logs on to one of these applications, the date and time are only recorded if it is the first access for this user this day. Other applications might record every access. The date and time in this message indicates the last recorded access. See z/OS Security Server RACF Security Administrator’s Guide for more information about how to configure applications to record daily statistics.

Information in the message includes hour, minute, second, day of week, month, day, and year.

The first time this message is issued for a user, the message is written **:**:** ON ***,*** **,****.

This message is routed to the RACF-defined user indicated by userid and is issued only when the INITSTATS option (specified on the SETROPTS command) is active.

ICH70002I YOUR PASSWORD [PHRASE] WILL EXPIRE IN xxx DAYS

Explanation: Your password or password phrase will expire within the specified number of days. RACF issues this message when the WARNING option on the PASSWORD keyword (specified on the SETROPTS command) is active.

One purpose of this message is to alert a batch user that the password on the JCL statements must be changed within xxx days.

ICH70003I YOU HAVE EXCEEDED THE MAXIMUM NUMBER OF RACF PASSWORD OR PASS PHRASE ATTEMPTS

Explanation: You have exceeded the number of consecutive unsuccessful password or password phrase attempts your installation allows.

System action: RACF revokes the user ID.

User response: To reactivated the user ID, see your RACF security administrator.

ICH70004I USER(accessor) GROUP(group-name) NAME(user-name) ATTEMPTED ’access-type’ ACCESS OF ENTITY ’resource-name’ IN CLASS ’class-name’ AT hh:mm:ss ON month day, year

Explanation: This message alerts a RACF user that an access violation has occurred against the indicated resource. This message is routed to the user specified in the NOTIFY field of the resource profile that denied the access.

Note: The lines of message text can appear in any order.

The message itself supplies the following information:

accessor
A user ID, job name, or started task name

group-name
A group of which the user is a member

access-type
The intended type of access, such as ALTER, CONTROL, UPDATE, EXECUTE, or READ

resource-name
A resource name, such as a data set name or a volume serial number

Note: The entity name is blank if the authorization check is done for a class in which there are no profiles, such as DIRAUTH.

class-name
One of the valid RACF class names.

The message also indicates the time and date of the violation.
ICH70005I Session attempt rejected. Reason code = xx, entity netid.luid1.luid2, profile profile-name, at hh:mm:ss on month, day, year

Explanation: An attempt by logical unit (LU) netid.luid1 to establish a session with the logical unit luid2 has been rejected for a security reason. The entity netid.luid1.luid2 was covered by profile profile-name. The message is routed to the user specified in the NOTIFY field of the profile.

System action: The session stops.

Operator response: Notify the RACF security administrator of the exact text of the message.

Problem Determination: Check the reason code in the message for one of the following values:

02 Local LU (luid1) session key will expire in 5 days or less.
03 Partner LU's (luid2) access has been revoked.
04 Session key does not match partner LU (luid2) session key.
05 Partner LU (luid2) stops the session because of a security reason.
06 Partner LU (luid2) verification required but no session key is defined on this system.
07 Possible security attack by partner LU (luid2).
08 Verification was not indicated by partner LU (luid2), but a session key exists on this system.
09 Verification was indicated by partner LU (luid2), but a session key does not exist on this system.
10 Failure because of SNA-security-related protocol error.
11 Failure because of profile change during verification.
12 The profile has an expired session key.

ICH70006I Userid userid associated with procedure [procname]!*UNKNOWN] has been revoked from [the system | group groupname]; verification for the procedure continues.

Explanation: During verification of a started procedure, user ID userid associated with procedure proiname was determined to be revoked from either the system or group groupname.

A value of *UNKNOWN for proiname indicates that the procedure name cannot be determined.

If proiname is blank, the procedure name is made up of at least one non-printable character, which might indicate an error in the procedure name specification.

System action: The revoked status of the user ID is ignored, and verification processing for the procedure continues.

User response: Notify your system programmer.

System programmer response:
- If the user ID is not intended to be revoked, use the RESUME operand of the ALTUSER command to reinstate the user ID. After the user ID is reinstated, this message will no longer appear.
- If the user ID is intended to be revoked, update the started procedures table (ICHRIN03) to associate another user ID with the procedure. The update will not take place until the next IPL, so this message might appear if the procedure is started again before the next IPL.

ICH70007I USER AUTHORITY CANNOT BE USED FOR THIRD-PARTY AUTHORIZATION CHECK FOR USER (userid) GROUP (groupid) BECAUSE THE EXECUTION NODE (nodeid) IS NOT LOCAL. UACC WILL BE USED.

Explanation: A third-party RACROUTE REQUEST=AUTH call was made specifying an execution node (nodeid). However, this execution node was not identified as a local node in the &RACLNDE profile in the RACFVARS class. The user's identity (userid) cannot be assumed to be valid at the current node, so the UACC authority for the protected resource is used. If that authority is not sufficient to allow access to the resource, message ICH408I is issued along with this message.

System action: RACF uses the UACC authority for the protected resource.

RACF Security Administrator Response: Check to see if the execution node is supposed to be local. If it is, make sure that the node is defined to the &RACLNDE profile in the RACFVARS class. Otherwise only the UACC authority for the protected resource can be obtained.
Chapter 4. IRR messages for RACF database initialization

This section lists the RACF messages issued by the IRRMIN00 utility during the initialization of the RACF database. The messages are routed to SYSOUT.

The format of the messages is:

IRR8nnn text

where:
IRR identifies the message as a RACF message.
8 identifies the RACF database initialization utility program (IRRMIN00).
nnn is the message serial number.
text is the text of the message.

Note: Some messages might also be issued to the console through WTO during RACF initialization. If so, these messages will be issued in upper case, rather than in mixed case. The message identifier will end with an I. Descriptor code will be 4, and routing codes 2 and 9.

IRR8000 Maximum number of template definitions exceeded.

Explanation: During initialization of the RACF database, more than 10 template definitions were found on the control card input from the data set defined by the SYSTEMP DD statement.

System action: Initialization of the RACF database stops.

Operator response: Report this message to your system programmer.

Programmer response: Ensure that no more than 10 template definitions exist in the data set defined by the SYSTEMP DD statement. Rerun the program.

Problem Determination: List the contents of the data set defined by the SYSTEMP DD statement to determine the cause of the problem.

IRR8001 Template is a duplicate. It is ignored.

Explanation: During initialization of the RACF database, two template definitions were found in the data set defined by the SYSTEMP DD statement with the same template number.

System action: Initialization of the RACF database continues using the first definition of the duplicate pair.

Operator response: Report this message to your system programmer.

Programmer response: If the second definition of the duplicate pair is the correct definition, delete the first definition and rerun the program.

Problem Determination: List the contents of the data set defined by the SYSTEMP DD statement to determine the cause of the problem.

IRR8002 RACF data base initialization complete.

Explanation: The RACF database has been successfully initialized.

System action: Processing continues.

IRR8003 Non-numeric character in numeric field of last statement.

Explanation: During the initialization of the RACF database, an invalid character was found in a numeric field of the previous input statement.

System action: Initialization of the RACF database stops.

Operator response: Report this message to your system programmer.

Programmer response: Ensure there are valid characters in the numeric fields and rerun the program.

Problem Determination: List the contents of the data set defined by the SYSTEMP DD statement to determine the cause of the problem.

IRR8004 RACF data base initialization terminated in error.

Explanation: Initialization of the RACF database has failed (as noted by a previous message).
**System action:** Initialization of the RACF database stops.

**Explanation:** Initialization of the RACF database has begun and template definitions will follow.

**System action:** Processing continues.

---

**IRR8006** Unable to open DD *ddname*

**Explanation:** The data set associated with the indicated *ddname* cannot be opened.

**System action:** Initialization of the RACF database stops.

**Operator response:** Report this message to your system programmer.

**Programmer response:** Ensure that the DD statement for the indicated data set is correct.

---

**IRR8007** End of file reached before $/END statement.

**Explanation:** During the initialization of the RACF database, an end-of-file condition was detected in the RACF templates before a $/END statement.

**System action:** Initialization of the RACF database continues.

**Operator response:** Report this message to your system programmer.

**Programmer response:** Verify the contents of the templates in the IRRMIN00 load module. If more template definitions were expected, the program must be rerun with the complete set of template definitions as input. If the problem continues, contact the IBM support center. If all template definitions are present and only the $/END statement is missing, the program need not be rerun.

---

**IRR8008** End of file reached before end of template definition.

**Explanation:** In attempting to initialize the RACF database, the end-of-file was encountered before a $/TEMPLATE statement was found.

**System action:** The RACF database is not initialized.

**Operator response:** Report this message to your system programmer.

**Programmer response:** Contact the IBM support center.

---

**IRR8009** Invalid JCL parameter: *parameter*

**Explanation:** The indicated parameter value is not a valid value for the NEW or UPDATE parameter. Only the first nine characters of the parameter value are listed.

**System action:** Updating of the RACF database stops.

**Operator response:** Report this message to your system programmer.

**Programmer response:** Correct the value specified on the NEW or UPDATE parameter and rerun the program.

---

**IRR8010** Unable to retrieve data base name.

**Explanation:** While attempting to retrieve the database name allocated by way of the SYSRACF DD statement, an error was encountered from the SVC 99 information retrieval function.

**System action:** Updating of the RACF database stops.

**Operator response:** Notify the system programmer.

**Programmer response:** Correct the SYSRACF DD statement and rerun the program.

---

**IRR8011** RACF data base header record is invalid.

**Explanation:** The RACF database initialization program found an invalid ICB (header) record in the RACF database while preparing to update the RACF database.

**System action:** Updating of the RACF database stops.

**Operator response:** Report this message to your system programmer.

**Programmer response:** If the RACF database was not previously formatted by way of this program with the PARM='NEW' specification on MVS or with the RACINITD EXEC on z/VM, then rerun the program with PARM='NEW'. If the RACF database is a version 1, release 1 or 2 database that is being updated, then run the RACF database verification utility program (IRRUT200) to determine which ICB field is in error.

**Problem Determination:** The validity check that caused the failure can result from an invalid ICB value for the number of templates or BAMs, or an invalid RBA (relative byte address). List the contents of the data set defined by the SYSRACF DD statement to determine the cause of the problem.

---

**IRR8012** RACF data base updates complete.

**Explanation:** The template update function of the RACF database initialization program has completed successfully.

**System action:** Processing continues.
IRR8013  RACF data base updates terminated in 
error.
Explanation: The template update function of the 
RACF database initialization program ended 
unsuccessfully as stated in a previous message.
System action: Updating of the RACF database stops.
Operator response: Report this message to your 
system programmer.
Programmer response: Respond to the previous 
message and rerun the program.

IRR8021  Dataset specified for UPDATE function 
is incorrect.
Explanation: The data set defined by the SYSRACF 
DD statement for the IRRMIN00 utility does not have a 
blocksize of 4096.
System action: Updating of the RACF database is 
ended.
Operator response: Notify the system programmer.
Programmer response: Make sure that the 
data set specified by the SYSRACF DD statement is a 
valid RACF data set. Rerun the IRRMIN00 utility.

IRR8021  The UPDATE parameter is not 
permitted while the system is in 
read-only mode.
Explanation: UPDATE attempts to update the data set 
templates. However, the database cannot be updated 
while the system is in read-only mode.
System action: The RACF database is not initialized. 
Utility processing stops.
System programmer response: You can do one of the 
following tasks:
• Run IRRMIN00 with a parameter of UPDATE from 
another system that is not in read-only mode.
• Issue RVARY DATASHARE to change the mode of all systems to data sharing mode and rerun the job.
• Issue RVARY NODATASHARE to change the mode of all systems to non-data sharing mode, then rerun the job.

IRR022 A coupling facility related error occurred during database UPDATE processing. Utility processing has ended abnormally.

Explanation: An error occurred when accessing the coupling facility. IRRMIN00 PARM=UPDATE has been run against an active data set while the system was in data sharing mode. The IRRMIN00 updates to DASD have been completed, but the ICB has not been updated in the coupling facility.

System action: IRRMIN00 processing ends abnormally.

System programmer response: Check the SYSPRINT. Also, check the information specified in message IRRX016I, which is issued to the system console.

You can do one of the following tasks:
• Rerun the job from the original system if it is still in data sharing mode.
• Rerun the job from another system in the RACF sysplex data sharing group, if that system is in data sharing mode.
• Issue RVARY NODATASHARE to change the mode of all systems to non-data sharing mode, then rerun the job.

IRR023 WARNING: The $/VERSION statement could not be found in the IRRTEMP1 template definition

Explanation: The RACF database initialization program was unable to find the template version statement.

System action: Updating of the RACF database continues.

Programmer response: Check the IRRTEMP1 DD statement to ensure that it points to the correct level of the templates.

IRR024I PARM=NEW specified for active RACF database. Processing stopped.

Explanation: You specified PARM=NEW when running IRRMIN00 but provided an active RACF database for the SYSRACF DD statement. This is not allowed, as it would destroy the contents of the active RACF database and cause system problems.

System action: IRRMIN00 stops processing and ends with RC=12.

User response: Either change to PARM=UPDATE or specify a different, inactive, RACF database as input to IRRMIN00 through the SYSRACF DD statement.

IRR025I PARM=UPDATE specified, but template update not required.

Explanation: You specified PARM=UPDATE when running IRRMIN00 but provided a RACF database using the SYSRACF DD statement that already has the latest level of the templates applied. See RACF database initialization utility program (IRRMIN00) in the z/OS Security Server RACF System Programmer's Guide for information about how RACF compares template versions.

System action: IRRMIN00 ends with RC=4 without making any changes to the database.

User response: If the correct STEPLIB is issued, no response is needed. To verify that the correct STEPLIB is issued, issue the SET LIST command, preceded by the RACF command character, to list the version of z/OS. Then search the IRRMIN00 load module for the IRRTEMP2 CSECT. You can then search this CSECT until rrrrrrr.aaaaaaa is located. You can also search the ICBTMPVR field in the database. This field (line 1 column 518) stores the actual rrrrrrr.aaaaaaa value.

IRR026I PARM=ACTIVATE specified; IRRMIN00 is preparing to activate the templates FMID or APAR rrrrrrrr.aaaaaaa.

Explanation: You specified PARM=ACTIVATE and IRRMIN00 is starting the process of activating the new level of templates from the master primary database on this system.

System action: None. IRRMIN00 continues processing and activating the templates on this system.

User response: None needed. This is an informational message.

IRR027I IRRMIN00 has finished activating the templates.

Explanation: You specified PARM=ACTIVATE and IRRMIN00 has activated the templates.

System action: IRRMIN00 finishes its processing and ends with RC=0.

User response: None needed. This is an informational message.

IRR028I IRRMIN00 cannot process PARM=ACTIVATE due to system error.

Explanation: You specified PARM=ACTIVATE when running IRRMIN00 but IRRMIN00 determined that an internal error has occurred in the MASTER address space and cannot proceed with template activation.

System action: IRRMIN00 stops processing and ends
with RC=12 without attempting to activate the
templates.

**User response:** Wait for an IPL; RACF will activate
the templates during the next IPL, and until then you
cannot activate new templates.

---

**IRR8029I**

*<contents of a template statement from
IRRTEMP2>.*

**Explanation:** RACF executed IRRMIN00 automatically
to process template definitions, but IRRMIN00 found
an error in the template definition and issued this
message to show the content of a template statement
that is in error. Another message will describe the
specific error that IRRMIN00 detected.

**System action:** None. IRRMIN00 continues processing.
However, IRRMIN00 will issue another message and
you might need to take additional action as indicated
in that message.

**User response:** None. See the other messages
produced by IRRMIN00.

---

**IRR8030I**

**PARM=ACTIVATE not supported.**

**Explanation:** You specified PARM=ACTIVATE but
either RACF is not active, or dynamic template
activation is not available on this system.

**System action:** IRRMIN00 stops processing and ends
with RC=12 without attempting to activate the
templates.

**User response:** Wait for an IPL; RACF will activate
the templates during the next IPL, and until then you
cannot activate new templates.

---

**IRR8031I**

**PARM=ACTIVATE specified, but there
is no master primary database active.**

**Explanation:** You specified PARM=ACTIVATE when
running IRRMIN00 but IRRMIN00 determined that
there was no active master primary RACF database to
read the templates from.

**System action:** IRRMIN00 stops processing and ends
with RC=12 without attempting to activate the
templates.

**User response:** If there currently is a master primary
RACF database that can be activated with RVARY, then
do so and rerun IRRMIN00. Otherwise, wait for an IPL;
RACF will activate the templates during the next IPL,
and until then you cannot activate new templates.

---

**IRR8032I**

**PARM=ACTIVATE specified, but the
level of the database templates: FMID or
APAR rrrrrrrrrrrrrrrrrrrrrrrrrrrrraanaaaa,
is not higher than
the level of templates on the system:
FMID or APAR rrrrrrrrrrrrrrrrrrrrrrrrrrrrraanaaaa.**

**Explanation:** You specified PARM=ACTIVATE when
running IRRMIN00 but system is already running with
a template level that is greater than or equal to those
found on the master primary RACF database.

**System action:** IRRMIN00 ends with RC=4 without
activating new templates.

**User response:** If the database template level is not
the same as the system level, then run the latest level
of IRRMIN00 PARM=UPDATE to update the database
templates and rerun the PARM=ACTIVATE. If the level
of the database templates is the same as the level of the
system templates, then no action is required.

---

**IRR8033I**

**Unable to establish ESTAE environment.**

**Return code from ESTAE is return-code**

**Explanation:** IRRMIN00 was unable to establish an
error recovery environment. Processing cannot continue
without such an environment.

**System action:** IRRMIN00 processing stops. No action
is taken.

**User response:** Notify your system programmer.

**System programmer response:** See “Problem
Determination”.

**Problem Determination:** For a description of the
ESTAE return code, see [*z/OS MVS Programming: Authorized Assembler Services Reference*](https://pubs.zos.mvs.com/zos/zos/mvs/zedtixg/).  

---

**IRR8034I**

**RACF Database updates must be done
with a z/OS V1R5.0 or later level of
IRRMIN00.**

**Explanation:** The templates on the database are z/OS
V1R5.0 (FMID HRF7708) or later level and can only be
updated with a version of the IRRMIN00 utility that is
that level or greater. The IRRMIN00 version you are
attempting to use to update the database is before
z/OS V1R5.0.

**System action:** IRRMIN00 processing stops. No action
is taken.

**User response:** Notify your system programmer.

**System Programmer Response:** Either run IRRMIN00
from the highest level of the z/OS V1R5.0 or later
systems that are sharing the RACF database, or have
the IRRMIN00 JCL STEPLIB to an APF authorized
library containing that highest level of IRRMIN00.
Chapter 5. IRR messages for the system operator

This section lists the messages with a prefix of IRR that go to the system operator. The format of these messages is:

\[ \text{IRR} \text{xnnt} \text{ text} \]

where:

- **IRR** identifies the message as a RACF message.
- **x** identifies the function issuing the message.
- **nn** is the message serial number.
- **t** is the type code (I = information, or A = action).
- **text** is the text of the message.

Routing and descriptor codes

The routing and descriptor codes for these messages are shown with the message explanations. When there is no destination indicated, the message is returned to the user. Only the messages that go to the operator console have a destination section.

Descriptor code descriptions

Descriptor codes indicate the significance of a message. Specifically, descriptor codes let the user know the status of the system itself or that of a specific task:

- Has it stopped processing?
- Is it waiting for another action to be completed?
- Or, is it continuing to process?

In addition, this code determines how the system displays and delete the message.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>System Failure</strong></td>
</tr>
<tr>
<td></td>
<td>The message indicates a catastrophic error. To continue, the operator must re-IPL the system or restart a major subsystem.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Immediate Action Required</strong></td>
</tr>
<tr>
<td></td>
<td>The message indicates that the operator must perform an action immediately. The message issuer can be in a wait state until the action is performed, or the system needs the action as soon as possible to improve performance. The task waits for the operator to complete the action.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When an authorized program issues a message with descriptor code 2, a DOM macro instruction must be issued to delete the message after the requested action is performed.</td>
</tr>
<tr>
<td>4</td>
<td><strong>System Status</strong></td>
</tr>
<tr>
<td></td>
<td>The message indicates the status of a system task or of a hardware unit.</td>
</tr>
<tr>
<td>5</td>
<td><strong>Immediate Command Response</strong></td>
</tr>
<tr>
<td></td>
<td>The message is issued as an immediate response to a system command. The response does not depend on another system action or task.</td>
</tr>
</tbody>
</table>
6  Job Status
The message indicates the status of a job or job step.

11 Critical Eventual Action Required
The message indicates that the operator must perform an action eventually, and the action is important enough for the message to remain on the display screen until the action is completed. The task does not wait for the operator to complete the action.

**Note:** Some RACF messages list a destination containing a descriptor code, but indicate that no routing codes are specified for the message. These messages are issued with a command and response token (CART) and console id (CONSID) to direct them to a specific console.

### Routing code descriptions
Routing codes send system messages to the consoles where they are to be displayed. To send a message to more than one console, RACF assigns more than one routing code to the message. For more information about message routing, see your MVS routing and descriptor codes manual.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Master Console Action</td>
</tr>
<tr>
<td></td>
<td>The message indicates a change in the status of the system. It requires action by the master console operator.</td>
</tr>
<tr>
<td>2</td>
<td>Master Console Information</td>
</tr>
<tr>
<td></td>
<td>The message indicates a change in the status of the system. It does not require action; rather, it alerts the master console operator to a condition that might require action.</td>
</tr>
<tr>
<td></td>
<td>This routing code is used for any message that indicates job status when the status is not requested specifically by an operator inquiry. It is also used for processor and problem program messages to the system operator.</td>
</tr>
<tr>
<td>9</td>
<td>System Security</td>
</tr>
<tr>
<td></td>
<td>The message gives information about security checking, for example, a request for a password.</td>
</tr>
<tr>
<td>11</td>
<td>Programmer Information</td>
</tr>
<tr>
<td></td>
<td>The message is intended for the problem programmer. This routing code is used only when the program issuing the message cannot route the message to the programmer by way of the system output (SYSOUT) data set. The message appears in the job log.</td>
</tr>
</tbody>
</table>

**Note:** Routing code 11 is ignored if specified for a multiple-line WTO macro instruction.

### VERIFY and VERIFYX messages

**IRR008I JOB FAILED. USER PARAMETER REQUIRED ON JOB STATEMENT.**

**Explanation:** A job was submitted with no user ID information specified or propagated from the submitter and the system requires jobs to run with RACF user IDs by way of the SETROPTS JES(BATCHALLRACF) or JES(XBMLRACF) options.

**System action:** The job stops. No steps are executed.

**User response:** Do one of the following tasks:
- Specify USER parameter on the JOB card
• Change JES(XBMALLRACF) to JES(NOXBMAALLRACF)
• Change JES(BATCHALLRACF) to JES(NOBATCHALLRACF)

Resubmit the job.

---

**IRR009I** JOB FAILED. OLD PASSWORD REQUIRED WITH NEW PASSWORD ON PASSWORD PARAMETER.

**Explanation:** The old password is missing on the PASSWORD parameter on the JOB statement.

**System action:** The job ends with no steps executed.

**User response:** Specify both the old password and the new password on the JOB card, PASSWORD=(old,new); and resubmit the job.

---

**IRR010I** USERID userid IS ASSIGNED TO THIS JOB.

**Explanation:** The user did not specify the USER parameter on the job card.

**System action:** The submitting user's user ID is assigned to this job. (This is normal for user ID propagation.) Processing continues. This message goes only to the job log.

**User response:** None.

---

**IRR011I** SECLABEL seclabel IS ASSIGNED TO THIS JOB.

**Explanation:** The user did not specify the SECLABEL parameter on the JOB card.

**System action:** The security label assigned to the job is the one the submitter is currently using. Processing continues.

**User response:** None.

---

**IRR012I** VERIFICATION FAILED. USER PROFILE NOT FOUND.

**Explanation:** There is no user profile in the RACF database for the user associated with this job.

**System action:** The external security manager has failed the request. The application decides whether to end the job or continue with an alternative method.

**User response:** If the application allows the job to continue, no action is required. Otherwise, specify a RACF-defined user on the USER parameter, or submit from a RACF-defined session.

---

**IRR013I** VERIFICATION FAILED. INVALID PASSWORD GIVEN.

**Explanation:** The password supplied was not contained in the user's profile.

**System action:** This depends on the application in use. It is checked out with RACF. In most cases, the system asks the user to provide a new password. In the case of a batch job, the job ends with no steps executed.

**User response:** Specify the correct password. For a batch job, it is in the PASSWORD parameter on the JOB card.

---

**IRR014I** VERIFICATION FAILED. EXPIRED PASSWORD GIVEN.

**Explanation:** The user's password has expired. A new password must be provided.

**System action:** The job ends with no steps executed.

**User response:** Specify a new password with the old expired one on the JOB card: PASSWORD=(old,new).

---

**IRR015I** VERIFICATION FAILED. NEW PASSWORD IS NOT VALID.

**Explanation:** The new password is not valid or is the same as the old password.

**System action:** The job ends with no steps executed.

**User response:** Specify a valid new password. For assistance with your installation's password rules and minimum password change interval, see your RACF security administrator.

---

**IRR016I** VERIFICATION FAILED BY RACF INSTALLATION EXIT.

**Explanation:** The job was failed by the RACINIT installation exit routine taken when the job was initiated.

**System action:** The job ends with no steps executed.

**User response:** Report this message to your RACF system programmer.

---

**IRR017I** VERIFICATION FAILED. USER IS REVOKED AT THE GROUP LEVEL.

**Explanation:** The group specified (which is either the default group or is specified on the job card) is a valid group for this user. However, the user's access to the group has been revoked.

**System action:** The job ends with no steps executed.

**User response:** Report this message to your RACF security administrator.

---

Chapter 5. IRR messages for the system operator 169
IRR018I

Explanation: The user is required to supply an operator ID card when entering the system. It is not possible to supply an OIDCARD with this batch job.

System action: The job ends with no steps executed.

User response: Specify a different user on the JOB card.
RACF processing messages

IRR401I  abend-code  ABEND DURING RACF PROCESSING OF  request-name REQUEST FOR ENTRY entry-name [IN CLASS class-name] [PRIMARY | BACKUP] RACF DATA SET SEQUENCE nnn, dsname] --or-- I/O ERROR AT RBA relative-byte-address DURING RACF PROCESSING OF request-name REQUEST FOR ENTRY entry-name [IN CLASS class-name] [PRIMARY | BACKUP] RACF DATA SET SEQUENCE nnn, dsname] --or-- RESTART KEY HIT DURING RACF PROCESSING OF request-name REQUEST FOR ENTRY entry-name [IN CLASS class-name] [PRIMARY | BACKUP] RACF DATA SET SEQUENCE nnn, dsname]

Explanation: An abend or an I/O error occurred during RACF processing, or the restart key was pressed.

relative-byte-address
The RBA (relative byte address) where the I/O error occurred.

request-name
The type of request the RACF manager was processing when the error occurred.

class-name
For resources other than DASD data sets, the class name of the resource. The 8-character class name and a hyphen precede the entry name zzz in the RACF database index. For example, the index name of TAPEVOL -T12345 is used to locate profile T12345 in class TAPEVOL.

dname and nnn
If more than one RACF database exists, dname and nnn indicate the database and sequence number affected.

System action: The indicated request to the RACF manager failed. RACF stops processing the request. An automatic RVARY might occur when there is an active backup and the device is varied offline or boxed.

Operator response: Save the exact text of this message and of any following RACF messages (particularly IRR413I), and report them to the system programmer or the RACF security administrator, or both.

Programmer response: If message IRR402I, IRR403I, or IRR404I does not follow this message, then a permanent error might exist in the RACF database. Perform the action as specified by the problem determination section for that message.

If an I/O error is occurring frequently on the RACF database, an alternate device can be considered for the next IPL.

If multiple extents were created for a new RACF database, this message is issued when the new database is used. Delete the database and rerun the IRRMIN00 utility to recreate it. Specify CONTIG and do not specify secondary space on the SPACE parameter in the JCL.

Problem Determination: If an abend occurred, do the following tasks:

• Get the abend code from this message. If the abend is 000, see other messages issued for this problem (such as ICH409I) for the abend code.

• Look for a description of the abend code in the following places:
  – Chapter 11, “RACF abend codes,” on page 393
  – z/OS MVS System Codes.

If you cannot find the abend code described in any of the above, see z/OS Security Server RACF Diagnosis Guide for information about diagnosing documentation errors and reporting documentation errors to IBM.

Diagnostic data is provided in the LOGREC data.

If an I/O error occurred, determine if the device or volume is malfunctioning. For a permanent I/O error, see the LOGREC data for diagnostic information. Also, see the section on failure during I/O operations on the RACF database in z/OS Security Server RACF System Programmer’s Guide.

If message IRR402I, IRR403I, or IRR404I follows this message, see “Problem Determination” for that message.

Destination: Descriptor code is 6 for x3E and x22 abends and 1 for all other abends. Routing codes are 9 and 11. The complete text of this message is sent only to the security console. Only IRR4011 abend-code ABEND DURING RACF PROCESSING is sent to the programmer.

IRR402I  BAM BLOCK AT RBA relative-byte-address MAY NOT REFLECT ACTUAL SPACE USAGE

Explanation: An error has occurred during RACF processing when attempting to allocate or deallocate...
space in the RACF database. The BAM block at the RBA (relative byte address) indicated in the message may not be accurate.

This message follows message IRR401I. If more than one RACF database exists, the database referred to in this message is the database named in the preceding IRR401I message.

**System action:** RACF processing of the request indicated in message IRR401I ends.

**Operator response:** Report this message to the system programmer or the RACF security administrator, or both, and save the message output.

**Problem Determination:** The control information in the RACF database may not be accurate. Execute the RACF database verification utility program IRRUT200 to determine the inconsistency between the BAM mappings and the actual space allocated.

If an inconsistency is found, use the BLKUPD command to correct the BAM blocks so they accurately reflect the space allocated. See [z/OS Security Server RACF Diagnosis Guide](#) for additional information about how to diagnose and correct problems with BAM blocks.

**Destination:** Descriptor code is 4. Routing code is 9.

---

**IRR403I INDEX MAY BE INVALID; LEVEL nn INDEX BEING PROCESSED FOR [ADDITION | DELETION] AT TIME OF FAILURE**

**Explanation:** An error occurred during RACF updating of the index in the RACF database. The level index being processed is indicated by *nn*. This message follows message IRR401I. If more than one RACF database exists, the database referred to in this message is the database named in the preceding IRR401I message.

**System action:** RACF stops processing the request indicated in message IRR401I.

**Operator response:** Report this message to the system programmer or the RACF security administrator, or both, and save the message output.

**Programmer response:** See “Problem Determination.”

**Problem Determination:** The control information in the RACF database might not be accurate. Execute the RACF database verification utility program IRRUT200 to determine if there is an inconsistency in the ICB and index structure. If an inconsistency is found, use the BLKUPD command to update the ICB so that it accurately reflects the contents of the index structure. See [z/OS Security Server RACF Diagnosis Guide](#) for additional information about how to diagnose and correct problems with the data set index.

**Destination:** Descriptor code is 4. Routing code is 9.

---

**IRR404I INSUFFICIENT SPACE ON RACF DATA SET [PRIMARY | BACKUP] RACF DATA SET SEQUENCE nnn, dsname**

**Explanation:** The RACF data set does not contain sufficient contiguous space to handle the RACF request. Either there is insufficient space available in the RACF data set or the available space has become too fragmented to satisfy the request.

If the RACF database is consisted of more than one data set, *dsname* with sequence number *nnn* is the data set that encountered the error.

**System action:** RACF stops processing the request.

**Operator response:** Report this message to the system programmer or the RACF security administrator, or both, and save the message output.

**Programmer response:** See “Problem Determination.”

**Problem Determination:** The control information in the RACF database might not be accurate. Execute the RACF database verification utility program IRRUT200 to determine if there is an inconsistency in the ICB and index structure. If an inconsistency is found, use the BLKUPD command to update the ICB so that it accurately reflects the contents of the index structure. See [z/OS Security Server RACF System Programmer's Guide](#) for additional information about how to diagnose and correct problems with the data set index.

**Destination:** Descriptor code is 4. Routing code is 9.
Problem Determination: Execute the RACF database verification utility program IRRUT200 to determine:

- The amount of available space in the RACF data set
- Whether significant fragmentation has occurred

If more space is needed, delete any unused profiles from the RACF data set. This might allow the request to succeed when you try again. If that is not sufficient, use the RACF database utility program IRRUT400 to rebuild the RACF data set and enlarge it if necessary. See z/OS Security Server RACF System Programmer’s Guide for information about the IRRUT200 and IRRUT400 utilities and for information about monitoring the RACF database to help you prevent future insufficient space conditions.

Destination: Descriptor code is 4. Routing codes are 2, 9, and 11.

IRR406I  RACF DATA SET INDEX FULL
[|PRIMAR|Y | BACKUP |] RACF DATA
SET SEQUENCE nnn, dsname]

Explanation: During RACF processing, an attempt was made to extend the index to another level, but the maximum number of index levels (10) had been reached.

If the RACF database is consisted of more than one data set, this message indicates which data set the error occurred on.

System action: RACF stops processing the request.

Operator response: Report this message to the system programmer or the RACF security administrator, or both, and save the message output.

Programmer response: See “Problem Determination.”

Problem Determination: Execute the RACF database verification utility program IRRUT200 to determine the error in the index tree in the RACF database.

If the IRRUT200 utility does not find the error, list the profile indicated in the message by entry-name, using the appropriate RACF command. For example, if the search was for user profiles, use the LISTUSER command. If CLASS was not specified on the SEARCH command, use the LISTDSD command. Look for error messages such as NO CONNECT ENTRY FOUND or invalid data in fields such as OWNER.

To correct any errors found, use the BLKUPD command. See z/OS Security Server RACF Diagnosis Guide for additional information about how to diagnose and correct problems with the data set index.

If you found no errors, it is possible that an in-storage overlay problem occurred, during which an index block was overwritten. Try solving the problem by flushing and rebuilding the in-storage buffers, by INACTIVATING and then REACTIVATING the appropriate RACF database(s) using the RVARY command. Be careful not to inadvertently drop the system into RACF FAILSOFT processing. You should also be aware that if you switch the primary database to the backup database, reactivate the old primary database and then switch back. There is a potential for the databases to be out of synchronization. Either do this procedure at a quiesced activity time or consider using the IRRUT200 utility, properly employed, to resynchronize them. See z/OS Security Server RACF Command Language Reference for details on RVARY usage and z/OS Security Server RACF System Programmer’s Guide for information about the IRRUT200 utility.

Destination: Descriptor code is 4. Routing codes are 9 and 11.

IRR407I  RACF DATA SET INDEX ERROR.
[|PRIMAR|Y | BACKUP |] RACF DATA
SET SEQUENCE nnn, dsname] SEARCH
ON ENTRY entry-name]

Explanation: An index error in the RACF database was detected while RACF was performing an index search for the entry indicated in the message. This message is issued if:

- During the index search, a block is found which is not an index block.
- The data pointed to by a level one index block is not the entry for the entry name indicated in the message.

If more than one RACF database exists, this message indicates which database the error occurred on.

System action: RACF stops processing the request.

Operator response: Report the exact text of this message to your system programmer or the RACF security administrator, or both.

System programmer response: See “Problem Determination.”

Problem Determination: Execute the RACF database verification utility program IRRUT200 to determine:
IRR410I RACF UNABLE TO BACK UP UPDATE OF entry-name BACKUP RACF DATA SET SEQUENCE mnn, dsname

Explanation: A failure occurred in attempting to duplicate on the backup RACF database an update performed in the corresponding primary database. The database is identified by:

mnn Database sequence number (1 to 255)
dname Database name.

System action: RACF has not duplicated the update operation. Processing continues.

Operator response: Notify system programmer.

Programmer response: See “Problem Determination.”

Problem Determination: If this message is preceded by message IRR401I, IRR405I, IRR406I, or IRR407I, the error was encountered on the backup database. Otherwise, the backup database was not in synchronization with its primary database. If the backup database was not in synchronization with the primary database, see z/OS Security Server RACF System Programmer’s Guide for information about the IRRUT200 and IRRUT400 utilities.

Destination: Descriptor code is 4. Routing code is 9.

IRR411I MAXIMUM PROFILE SIZE EXCEEDED. profile-name NOT ALTERED.

Explanation: During RACF processing, an attempt was made to expand profile profile-name. The profile has reached the maximum output size that RACF can handle (65 535 bytes); the profile cannot be made larger.

Note: Although some profiles can be larger for repeat groups, the maximum output length remains at 65 535 bytes.

System action: RACF stops processing the request.

Operator response: Report this message to the system programmer or the RACF security administrator, or both, and save this output.

Programmer response: Profile has reached the maximum size allowed. If possible, decrease the size of the profile; if that is not possible, you must split the profile. For example, you can split a group with too many users into several smaller groups.

Destination: Descriptor code is 4. Routing code is 9.

IRR413I RACF MANAGER REQUEST ID WAS request-id

Explanation: This message contains additional information to help determine the cause of an IRR401I error message. This message is issued only after an IRR401I message. The request-id field contains an ID that can help the IBM support center determine the cause of the problem.

System action: See message IRR401I.

Operator response: See message IRR401I.

Programmer response: message IRR401I.

Destination: Descriptor code is 4. Routing codes are 4 and 13.

IRR416I RACF DETECTED AN INVALID NON-EGN DATASET PROFILE NAME. PROFILE profile-name DOES NOT PROTECT THE INTENDED RESOURCES.

Explanation: RACF detected a profile that was added before the enablement of Enhanced Generic Names (EGN) and that cannot be interpreted as intended under EGN rules. This message identifies the non-EGN generic data set profile name. Under EGN rules, the profile may not protect the resources that it was defined to protect. If this message is issued during processing of a SEARCH or LISTDSD GENERIC request, bad profile names (particularly names 43 and 44 characters in length) might also have been displayed and the output should be considered unreliable.

For example, suppose the following six generic data set profiles were defined before turning EGN on:

1 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.D.*'
2 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.XX.D.DD*'
3 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.D.*'
4 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.XX.D.DD*'
5 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.XX.D.D.*'
6 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.XX.D.DD*'

Then EGN was enabled and three more generic data set profiles were defined:

7 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.U.**'
8 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.US.**'
9 ADDSD 'IBMUSER.IBMUSER.IBMUSER.IBMUSER.USE.**'

Then EGN was enabled and three more generic data set profiles were defined:

A subsequent SEARCH request would display the following information:
RACF command processing may have caused the IRR416I message to be issued more than once. However, any time it is issued during a command invocation, the command output must be considered unreliable. In the example above, changes in EGN rules might have caused RACF to incorrectly interpret non-EGN profiles (1) and (2) as SEARCH profiles (A) and (B). These profiles no longer cover the intended resources. Even though names (D) and (E) appear correct, with no additional characters at the end, they also do not cover the intended resources and cause IRR416I messages to be issued. EGN profiles (7), (8), and (9) were correctly displayed by SEARCH as (C), (F), and (I). Profiles (G) and (H) follow the same rules under non-EGN and EGN, so they actually protect what they were intended to protect.

**System action:** RACF processing of the request continues.

**Operator response:** Report this message to the system programmer or the RACF security administrator and save the message output.

**Programmer response:** See "Problem Determination."

**Problem Determination:** This message identifies the bad profile.

An EGN profile, possibly less specific, can be defined to protect the wanted resources; however, the original bad non-EGN profile must still be deleted to prevent further IRR416I messages.

To delete bad profiles:

1. Use SETROPTS NOEGN to temporarily disable EGN. During this time, there should be no other system activity, in order to prevent the creation of generic profiles that can result in additional problems. Under normal circumstances, it is not recommended that EGN be turned off after it is turned on.
2. Use SEARCH GENERIC CLIST NOMASK NOLIST to create a CLIST containing generic data set profile names.
3. Edit the CLIST, to find 42- and 43-character names ending in ".*".
4. Delete the profiles found.
5. Use SETROPTS EGN to re-enable EGN.
6. Define profiles according to EGN rules that protect the resources intended to be protected by the non-EGN profile names.

**Destination:** Descriptor code is 4. Routing codes are 9 and 11. Routing code 11 is only used when a TSO environment is not in effect.

---

**IRR417I UNABLE TO COMMUNICATE WITH THE RACF SUBSYSTEM. IEFSSEQ RETURN CODE IS return-code.**

**Explanation:** A RACF function requiring the RACF subsystem was unable to communicate with the subsystem. Report this message to your system programmer. The possible functions, and the effect of the failure are as follows:

1. **RRSF password synchronization**
   
   RACF attempted to process a password change request for a user. The password change has been made on this system's RACF database. However, if associations exist with another user on this or a remotely connected system, the passwords are not synchronized.

2. **PKCS #7 enveloping**
   
   RACF attempted to process a password or password phrase change request for a user. The RACF database on this system has been updated accordingly. However, a PKCS #7 envelope was not created for this update. An existing envelope might exist for the user's previous password or password phrase.

3. **LDAP event notification**
   
   A RACF profile was changed but the LDAP change log entry was not created. Applications that require the change log entry for RACF event notifications do not know about this profile change.

4. **IRRUT200 Activation**
   
   PARM=ACTIVATE was specified on IRRUT200. This message results in...
5. **Kerberos Key Generation**

RACF attempted to process a password or password phrase change request for a user. The RACF database on this system has been updated accordingly. However, a Kerberos key was not created for this update. An existing key might exist for the user’s previous password or password phrase.

**System action:** The system continues processing.

**System programmer response:** The return code indicated in this message reflects the return code from the MVS IEFSSREQ subsystem interface. See [z/OS MVS Using the Subsystem Interface](https://www.ibm.com/docs/en/zos/2.4.0?topic=using-subsystem) for a list of the possible values and their explanations.

Ensure that the RACF subsystem has not been shut down. A return code of 8 or 12 indicates an installation or RACF subsystem configuration. See [z/OS Security Server RACF System Programmer’s Guide](https://www.ibm.com/docs/en/ racf-system-programmers-guide) for configuration considerations for the RACF subsystem.

**Destination:** Descriptor code is 3. Routing codes are 9 and 11.

---

**IRR418I**

RACF PRODUCT DISABLED:

(COMMAND | UTILITY | IRRSSM00 | IRRSSI00 | IRRDP00) ENDED.

**Explanation:** This system is running z/OS Version 1 Release 2 or higher. The RACF initialization process made a registration check based on the IFAPRDxx member in SYS1.PARMLIB. This message implies that:

- The RACF product was not enabled
- RACF initialization did not continue
- Control was given to a RACF command processor, RACF utility, or that initialization was attempted for the RACF subsystem (IRRSSM00 or IRRSSI00) or for RACF’s dynamic parse (IRRDP00)

**Note:** This message can be sent as:

- A TSO message
- Batch job output
- A console message

**System action:** Because RACF is not enabled, the respective process ends. The return code for RACF utilities failing in this way is X’20’ (decimal 32).

**Destination:** Descriptor code is 11. Routing codes are 1 and 9.
**IRRDP100 command messages**

**IRR545I** IRRDP100 FAILED BECAUSE IT IS NOT A TSO-AUTHORIZED COMMAND

**Explanation:** This message is issued when the IRRDP100 UPDATE command is issued from a started task (for example, during IPL), but the IRRDP100 command is not defined as an authorized command in the IKJTSOxx parameter library member.

**System action:** RACF processing continues normally, except that users cannot work with profile segments (such as TSO or DFP segments). This affects both RACF command users and RACF ISPF panel users.

**Operator response:** Report this message to your system programmer.

**System programmer response:** Ensure that the IRRDP100 command is defined as an authorized command in the IKJTSOxx parameter library member.

If the problem persists, call your IBM support center.

---

**IRR546I** jobname FAILED. SAVE JOB LOG AND CONTACT SYSTEM SUPPORT

**Explanation:** This message is issued when the IRRDP100 UPDATE command is issued from a started task (for example, during IPL), and then a problem occurs. The jobname is the name of the job used to run dynamic parse.

**System action:** RACF processing continues normally, except that users cannot work with profile segments (such as TSO or DFP segments). This affects both RACF command users and RACF ISPF panel users.

**Operator response:** Report this message to your system programmer.

**System programmer response:** Check the job log of the started task for other messages that might be related to this problem. Find out what was wrong, correct the problem, and re-IPL.

---

**RACROUTE REQUEST=AUTH VLF messages**

**IRR803I** VLF IS NOT ACTIVE. POSSIBLE RACF PERFORMANCE IMPACT

**Explanation:** This message appears when VLF is inactive and RACF is doing group authority checking. RACF uses VLF to store group tree information for improving performance.

**System action:** RACF continues processing without using VLF. The result of group authority checking should be the same whether VLF is active or not.

**Operator response:** Use operation procedures for your installation to decide whether to activate VLF. The command S VLF, SUB=MSTR starts the VLF, and VLF uses the COFVLF00 PARMLIB member as the default. The command STOP VLF deactivates VLF. See z/OS Security Server RACF System Programmer’s Guide for detailed VLF usage information.

- VLF might have become active subsequent to the issuance of this message. The results of command D A,VLF includes GTS object names DIRRGTS & CIRRGTS as data spaces if VLF is active and being used for group tree storage.

**Destination:** Descriptor code is 4. Routing code is 1.

**IRR804I** RACF VLF CLASS IRRGTS NOT DEFINED IN COFVLFxx PARMLIB.

**Explanation:** This message displays when VLF is active but the VLF class IRRGTS is not defined in the COFVLFxx parameter library member. Therefore, GTS (group trees in VLF storage) cannot be activated in RACF. It affects the RACF performance during group authority checking.

**System action:** RACF continues processing without GTS. The result of group authority checking should be the same no matter whether GTS is active or not.

**Operator response:** Use the installation procedures to decide whether to activate GTS. If the decision is to have GTS active, update the COFVLFxx PARMLIB member to specify that the VLF class name is IRRGTS and its major name is GTS. Add the following two lines to the COFVLFxx parameter library member:

```
CLASS NAME(IRRGTS) /* RACF GTS Feature */
EMAJ(GTS) /* Major Name */
```

After updating the COFVLFxx PARMLIB, you must activate GTS. One way to make GTS active is to stop VLF, and start it again with the updated COFVLFxx parameter library member.

**Destination:** Descriptor code is 4. Routing code is 1.
### RACROUTE REQUEST=VERIFY NJE messages (Part 1)

#### Note on NJE Messages
See message IRR815I for an additional NJE operator message.

<table>
<thead>
<tr>
<th>Message</th>
<th>Explanation</th>
<th>System action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRR805I</td>
<td><strong>IDENTITY IS PROPAGATED FOR THE</strong> <strong>UNKNOWN USER FROM TRUSTED NODE</strong> <strong>node-name</strong>.</td>
<td><strong>Explanation:</strong> This informational message is sent to the security console when a job is received from an unknown user on a trusted node. The NODES profile lookup for this submitter resulted in a UACC that allowed propagation of the NJE unknown user, set by SETROPTS JES(NJEUSERID(userid)). Propagation of this submitter is not possible. This situation can occur when a job is sent across nodes by an external physical reader such as a card reader. See z/OS Security Server RACF Security Administrator's Guide for details on the NODES profile lookup. This message occurs only once per IPL; however, an SMF record is cut for every occurrence. <strong>System action:</strong> The job is allowed to run. If a user ID is specified, a password is required and no propagation takes place. If a user ID is not specified, the job runs according to the setting on the SETROPTS JES(BATCHALLRACF) command. See z/OS Security Server RACF Security Administrator's Guide for information about using the BATCHALLRACF operand.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message</th>
<th>Explanation</th>
<th>System action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRR806I</td>
<td><strong>PROFILE profile-name IN THE NODES CLASS WAS USED TO TRANSLATE</strong> <strong>USER userid-1 TO userid-2.</strong></td>
<td><strong>Explanation:</strong> This informational message is sent to the security console when a user ID is translated for NJE (network job entry). The <strong>profile-name</strong> is the actual profile used to do the translation. To determine which ENTITY was built, see z/OS Security Server RACF Security Administrator's Guide for information about NODES profiles. <strong>System action:</strong> Processing continues with <strong>seclabel-2</strong> as the current security label.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message</th>
<th>Explanation</th>
<th>System action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRR807I</td>
<td><strong>PROFILE profile-name IN THE NODES CLASS WAS USED TO TRANSLATE</strong> <strong>SECLABEL seclabel-1 TO seclabel-2.</strong></td>
<td><strong>Explanation:</strong> This informational message is sent to the security console when a security label is translated for NJE (network job entry). The <strong>profile-name</strong> is the actual profile used to do the translation. To determine which ENTITY was built, see z/OS Security Server RACF Security Administrator's Guide for information about NODES profiles. <strong>System action:</strong> Processing continues with <strong>seclabel-2</strong> as the current security label.</td>
</tr>
</tbody>
</table>

Note: When userid-2 is “&USER”, it is possible for an additional IRR806I message to be issued, because a second NODES lookup is done. See z/OS Security Server RACF Security Administrator's Guide for information about &USER. **System action:** Processing continues with the authority of userid-2.
RACF user ID and group ID mapping messages

IRR809I  VLF CLASS IRRUMAP NOT IN COFVLF:xx PARMLIB OF VLF.
Explanation: VLF is active, but the VLF class IRRUMAP is not defined in the COFVLF:xx parmlib member. Therefore, the UMAP function of RACF cannot be activated. The performance of UID-to-user ID mapping is affected because a search of the RACF database must be performed to retrieve this information.

System action: RACF continues processing without using VLF for the UMAP function. The results of the UID-to-user ID mapping are not affected.

System programmer response: Use the installation procedures to decide whether to activate the UMAP function. If the decision is to have UMAP active, update the COFVLF:xx parmlib member. For the procedure for this, see z/OS Security Server RACF System Programmer’s Guide.

Destination: Descriptor code is 4. Routing code is 1.

IRR810I  VLF CLASS IRRGMAP NOT IN COFVLF:xx PARMLIB OF VLF.
Explanation: VLF is active, but the VLF class IRRGMAP is not defined in the COFVLF:xx parmlib member. Therefore, the GMAP function of RACF cannot be activated. The performance of GID-to-group name mapping is affected because a search of the RACF database must be performed to retrieve this information.

System action: RACF continues processing without using VLF for the GMAP function. The results of the GID-to-group name mapping are not affected.

System programmer response: Use the installation procedures to decide whether to activate the GMAP function. If the decision is to have GMAP active, update the COFVLF:xx parmlib member. For the procedure for this, see z/OS Security Server RACF System Programmer’s Guide.

Destination: Descriptor code is 4. Routing code is 1.

Dynamic started task messages

IRR812I  PROFILE profile-name [(G)] IN THE STARTED CLASS WAS USED TO START member-name [WITH JOBNAME jobname].
Explanation: An MVS START command was processed. The STARTED class is active and SETROPTS RACLISTed. The indicated profile in the STARTED class has an STDATA segment that specifies TRACE(YES).

Operator response: Notify the system programmer or security administrator. Tell them the profile name, member name, and job name (if any) contained in the message text.

System programmer response: The security administrator responsible for profiles in the STARTED class has requested that message IRR812I be issued whenever the indicated profile is used when processing a START command. The administrator should be informed that this message has occurred.

Destination: Descriptor code is 6. Routing code is 9.

IRR813I  NO PROFILE WAS FOUND IN THE STARTED CLASS FOR member-name [WITH JOBNAME jobname]. RACF WILL USE ICHRIN03.
Explanation: An MVS START command was processed and the STARTED class is active. One of the following problems occurred:

- The STARTED class is SETROPTS RACLISTed, but no profile was found to assign security information for the procedure or job being started.
- A profile to assign security information for the procedure or job being started has been defined, but the STARTED class has not been SETROPTS RACLISTed, or has not been SETROPTS RACLIST REFRESHed on the system where the START command was issued.

System action: RACF uses the information in the started procedures table (ICHRIN03) to assign security information for this started procedure or job.

Operator response: Notify the system programmer or security administrator. Tell them the member name and job name (if any) contained in the message text.

System programmer response: Do one of the following tasks:

- The security administrator responsible for profiles in the STARTED class has not defined a profile to be used when starting the indicated procedure or job. Inform the administrator that this message has occurred so a profile can be defined, if one is wanted.
- Profiles exist or have been defined in the STARTED class for the indicated procedure or job, but the security administrator has not SETROPTS RACLISTed or SETROPTS RACLIST REFRESHed the STARTED class. The administrator should be informed that this message occurred so the STARTED class can be SETROPTS RACLISTed or SETROPTS RACLIST REFRESHed.
IRR814I • IRR900A

Destination: Descriptor code is 6. Routing code is 9.

IRR814I PROFILE profile-name [(G)] IN THE STARTED CLASS DID NOT ASSIGN A USERID FOR member-name [WITH JOBNAME jobname]. RACF WILL USE ICHRIN03.

Explanation: An MVS START command was processed. The STARTED class is active and SETROPTS RACLISTed. The profile that matches the procedure name (and job name, if any) did not assign a user ID to be used for the procedure or job being started.

System action: RACF uses the information in the started procedures table (ICHRIN03) to assign security information for this started procedure or job.

Operator response: Notify the system programmer or security administrator. Tell them the profile name, member name, and job name (if any) contained in the message text.

System programmer response: The security administrator responsible for profiles in the STARTED class has defined an incomplete profile to be used when starting the indicated procedure or job. The administrator should be informed that this message has occurred so the profile can be corrected.

Destination: Descriptor code is 6. Routing code is 9.

RACROUTE REQUEST=VERIFY NJE messages (Part 2)

Note on NJE Messages
Additional NJE operator messages begin with message IRR805I.

IRR815I PROFILE profile-name IN THE NODES CLASS WAS USED TO TRANSLATE GROUP group-1 TO group-2.

Explanation: This informational message is sent to the security console when a group ID is translated for NJE (network job entry). The profile-name is the actual profile used to do the translation. To determine which entity was built, see z/OS Security Server RACF Security Administrator's Guide for information about NODES profiles.

Note: When group-2 &DFLTGRP, the user's default group is used for purposes of verification.

System action: Processing continues with the authority of group-2.

VLF cache messages

IRR816I VLF CLASS 'IRRSMAP' NOT DEFINED IN COFVLFx PARMLIB OF VLF.

Explanation: VLF is active but the VLF class IRRSMAP is not defined in the COFVLFx PARMLIB member. Performance during the creation of user security packets (USP) is impacted.

System action: RACF continues processing without using VLF for the SMAP function. The results of the initUSP callable service to create user security packets are not affected.

System programmer response: Use the installation procedures to decide whether to activate the SMAP function. If you decide to activate the function, update the COFVLFx PARMLIB member. To see a procedure for this, see z/OS Security Server RACF System Programmer's Guide.

Destination: Descriptor code is 4. Routing code is 1.

IBM DB2 external security module for RACF

IRR900A RACF/DB2 EXTERNAL SECURITY MODULE FAILED TO INITIALIZE FOR DB2 SUBSYSTEM subsystem-name BECAUSE CLASS classname COULD NOT BE RACLISTED. RACROUTE RETURN CODE return_code, RAC RETURN CODE return_code, REASON CODE reason_code.

Explanation: The IBM DB2 external security module for RACF initialization function for DB2 subsystem subsystem-name attempted to RACLIST class classname using RACROUTE REQUEST=LIST,ENVIR=CREATE,GLOBAL=YES. If this is DB2 data sharing, subsystem-name is the group attach name. Otherwise, it is the DB2 subsystem. The RACROUTE request failed with the return and reason codes provided in the message text. The return and reason codes are shown in hexadecimal format.

System action: See System Action for message IRR912I or IRR913I.

Operator response: Contact the system programmer.
System programmer response: Use the RACROUTE return code and RACF return and reason codes to determine the cause of the failure. After you correct the problem, restart DB2.

Destination: Descriptor code is 2. Routing codes are 1 and 9.

IRR901A RACF/DB2 EXTERNAL SECURITY MODULE FAILED TO INITIALIZE FOR DB2 SUBSYSTEM subsystem-name BECAUSE NO ACTIVE DB2 RELATED CLASSES WERE FOUND.

Explanation: The IBM DB2 external security module for RACF initialization function for subsystem subsystem-name determined that no classes for the indicated DB2 subsystem are active. If this is DB2 data sharing, subsystem-name is the group attach name. Otherwise, it is the DB2 subsystem.

System action: See System Action for message IRR912I or IRR913I.

Operator response: Contact your security administrator.

RACF Security Administrator Response: Activate the wanted classes for the indicated DB2 subsystem and restart DB2.

Destination: Descriptor code is 2. Routing codes are 1 and 9.

IRR902A RACF/DB2 EXTERNAL SECURITY MODULE FAILED TO INITIALIZE FOR DB2 SUBSYSTEM subsystem-name BECAUSE THE INPUT ACEE WAS (MISSING | NOT VALID).

Explanation: The IBM DB2 external security module for RACF initialization function for subsystem subsystem-name determined that the input DB2 subsystem ACEE was either not valid or missing. If this is DB2 data sharing, subsystem-name is the group attach name. Otherwise, it is the DB2 subsystem.

System action: See System Action for message IRR912I or IRR913I.

Operator response: Contact the DB2 system programmer.

System programmer response: Contact the IBM support center.

Destination: Descriptor code is 2. Routing codes are 1 and 9.

IRR903A RACF/DB2 EXTERNAL SECURITY MODULE FAILED TO INITIALIZE FOR DB2 SUBSYSTEM subsystem-name BECAUSE RACF WAS NOT ACTIVE.

Explanation: The IBM DB2 external security module for RACF initialization function for subsystem subsystem-name determined that RACF is not active on this system. If this is DB2 data sharing, subsystem-name is the group attach name. Otherwise, it is the DB2 subsystem.

System action: See System Action for message IRR912I or IRR913I.

Operator response: Contact the RACF system programmer.

Problem Determination: Issue the RVARY LIST command to determine RACF status.

System programmer response: Determine why RACF is inactive. After you correct the problem, activate RACF and restart DB2.

Destination: Descriptor code is 2. Routing codes are 1 and 9.

IRR904I RACF/DB2 EXTERNAL SECURITY MODULE INITIALIZED WITH WARNINGS FOR DB2 SUBSYSTEM subsystem-name BECAUSE A DEFAULT ACEE COULD NOT BE CREATED. RACROUTE RETURN CODE return_code, RACF RETURN CODE return_code, REASON CODE reason_code.

Explanation: The IBM DB2 external security module for RACF initialization function for subsystem subsystem-name attempted to create a default ACEE to use in subsequent authority checking when no ACEE is provided. If this is DB2 data sharing, subsystem-name is the group attach name. Otherwise, it is the DB2 subsystem.

The attempt to create the ACEE using RACROUTE REQUEST=VERIFY,ENVIR=CREATE failed with the return and reason codes provided in the message text. The return and reason codes are shown in hexadecimal format.

System action: Processing continues and the IBM DB2 external security module for RACF is used for subsequent authority checking if DB2 provides an ACEE. If no ACEE is provided, requests are deferred to DB2.

Operator response: Contact the DB2 system programmer.

System programmer response: Use the RACROUTE return code and RACF return and reason codes to determine the cause of the failure. After you correct the problem, restart DB2.

Destination: Descriptor code is 12. Routing codes are 2, 9, and 10.
IRR905I  IRR908I

IRR905I  RACF/DB2 TERMINATION FUNCTION COMPLETED WITH WARNINGS FOR DB2 SUBSYSTEM subsystem-name BECAUSE CLASS classname COULD NOT BE UN-RACLISTED. RACROUTE RETURN CODE return_code, RACF RETURN CODE return_code, REASON CODE reason_code.

Explanation: The IBM DB2 external security module for RACF termination function for subsystem subsystem-name attempted to delete RACLISTed profiles for class classname. If this is DB2 data sharing, subsystem-name is the group attach name. Otherwise, it is the DB2 subsystem.

The attempt to delete the profiles using RACROUTE REQUEST=LIST,ENVIR=DELETE failed with the return and reason codes provided in the message text. The return and reason codes are in hexadecimal format.

System action: The termination function continues processing. Resources are cleaned up when processing completes. This does not impact RACF authorization checking when DB2 is restarted.

Operator response: Contact the DB2 system programmer.

System programmer response: Use the RACROUTE return code and the RACF return and reason codes to determine the cause of the failure. After you correct the problem, restart DB2.

Destination: Descriptor code is 12. Routing codes are 2, 9, and 10.

IRR907I  RACF/DB2 TERMINATION FUNCTION COMPLETED WITH WARNINGS FOR DB2 SUBSYSTEM subsystem-name BECAUSE THE DEFAULT ACEE WAS [MISSING  NOT VALID].

Explanation: The IBM DB2 external security module for RACF termination function for the subsystem subsystem-name determined that the input DB2 subsystem ACEE was either not valid or missing. If this is DB2 data sharing, subsystem-name is the group attach name. Otherwise, it is the DB2 subsystem.

System action: For exit termination, the IBM DB2 external security module for RACF is not able to complete its termination function. This should not impact RACF authorization checking when DB2 is restarted.

Operator response: Contact the DB2 system programmer.

System programmer response: Use the RACROUTE return code and the RACF return and reason codes to determine the cause of the failure. After you correct the problem, restart DB2.

Destination: Descriptor code is 12. Routing codes are 2, 9, and 10.

IRR906I  RACF/DB2 TERMINATION FUNCTION COMPLETED WITH WARNINGS FOR DB2 SUBSYSTEM subsystem-name BECAUSE THE DEFAULT ACEE COULD NOT BE DELETED. RACROUTE RETURN CODE return_code, RACF RETURN CODE return_code, REASON CODE reason_code.

Explanation: The IBM DB2 external security module for RACF termination function for the subsystem subsystem-name attempted to delete the default ACEE used by the external security module. If this is DB2 data sharing, subsystem-name is the group attach name. Otherwise, it is the DB2 subsystem.

The attempt to delete the ACEE by using RACROUTE REQUEST=VERIFY,ENVIR=DELETE failed with the return and reason codes provided in the message text. The return and reason codes are in hexadecimal format.

System action: The termination function continues processing and resources are cleaned up when processing completes. This does not impact RACF authorization checking when DB2 is restarted.

Operator response: Contact the DB2 system programmer.

System programmer response: Use the RACROUTE return code and the RACF return and reason codes to determine the cause of the failure. After you correct the problem, restart DB2.

Destination: Descriptor code is 12. Routing codes are 2, 9, and 10.

IRR908I  RACF/DB2 EXTERNAL SECURITY MODULE FOR DB2 SUBSYSTEM subsystem-name HAS A MODULE VERSION OF module-version AND A MODULE LENGTH OF module-length.

Explanation: The IBM DB2 external security module for RACF initialization function for subsystem subsystem-name has determined the version and length of the RACF/DB2 external security module for subsystem subsystem-name. If this is DB2 data sharing, subsystem-name is the group attach name. Otherwise, it is the DB2 subsystem. module-version is the FMID or APAR number associated with the module. module-length is the hexadecimal length of all CSECTs contained in the module.

System action: The RACF external security module continues.

Destination: Descriptor code is 4. Routing codes are 9 and 10.
IRR909I RACF/DB2 EXTERNAL SECURITY MODULE FOR DB2 SUBSYSTEM 

subsystem-name IS USING OPTIONS: 

&CLASSOPT= classopt &CLASSNMT= classnmt &CHAROPT= charopt 
&ERROROPT= erroropt &PCELLCT= pcelct &SCELLCT= scelct 

Explanation: The IBM DB2 external security module for RACF initialization function for subsystem 

subsystem-name lists the options that are being used for the RACF/DB2 external security module. If this is DB2 data sharing, subsystem-name is the group attach name. Otherwise, it is the DB2 subsystem. For an explanation of the options, see [z/OS Security Server RACF System Programmer’s Guide](https://www.ibm.com/support/docview.zhtml?docid=581411). 

System action: The RACF external security module continues. 

Destination: Descriptor code is 4. Routing codes are 9 and 10. 

IRR910I RACF/DB2 EXTERNAL SECURITY MODULE FOR DB2 SUBSYSTEM 

subsystem-name INITIATED RACLST FOR CLASSES: {classname-list | * NONE *} 

Explanation: The IBM DB2 external security module for RACF initialization function for DB2 subsystem 

subsystem-name issued a RACROUTE REQUEST=LIST,GLOBAL=YES macro for classes 

classname-list as defined in the object table in the RACF/DB2 external security module. If “* NONE *” is displayed, an error occurred before the initialization function can issue RACROUTE REQUEST=LIST for any class. If this is DB2 data sharing, subsystem-name is the group attach name. Otherwise, it is the DB2 subsystem. 

System action: The RACF/DB2 external security module continues. 

Destination: Descriptor code is 4. Routing codes are 9 and 10. 

IRR911I RACF/DB2 EXTERNAL SECURITY MODULE FOR DB2 SUBSYSTEM 

subsystem-name SUCCESSFULLY RACLISTED CLASSES: {classname-list | * NONE *} 

Explanation: The IBM DB2 external security module for RACF initialization function for DB2 subsystem 

subsystem-name lists the classes for which the RACROUTE REQUEST=LIST,GLOBAL=YES macro was successful. If “* NONE *” is displayed, no classes were RACLISTed successfully. See message IRR910I to determine which classes the RACF/DB2 external security module attempted to use. The class list displayed in IRR911I might be a valid subset of the classes listed in message IRR910I. See [z/OS Security Server RACF Security Administrator’s Guide](https://www.ibm.com/support/docview.zhtml?docid=581411) for more information about initializing the RACF/DB2 external security module. 

System action: The RACF/DB2 external security module continues. 

Destination: Descriptor code is 4. Routing codes are 9 and 10. 

IRR912I NATIVE DB2 AUTHORIZATION IS USED. 

Explanation: RACF is not being used to control access to DB2 resources. This message is preceded by other messages that describe why RACF is not being used for access control decisions. 

System action: None. All subsequent access control decisions are made by DB2 using DB2’s native security mechanism. 

Operator response: Follow the Operator Response for the message that preceded this message. 

Destination: Descriptor code is 2. Routing codes are 1 and 9. 

IRR913I DB2 SUBSYSTEM TERMINATION REQUESTED. 

Explanation: RACF has requested that the DB2 subsystem be terminated. This message is preceded by another message which describes why this request has been made. 

System action: RACF has requested that the DB2 subsystem terminate. 

Operator response: Follow the Operator Response for the message that preceded this message. 

Destination: Descriptor code is 2. Routing codes are 1 and 9. 

IRR914I DSNX@XAC has been invoked with a DB2 VxRxMx parameter list 

Explanation: The IBM DB2 external security module for RACF was invoked from a DB2 V8 system. However, the parameter list that was passed was for another version of DB2. This mismatch of DB2 version and level of RACF/DB2 external security module is not allowed. 

System action: If IBM DB2 external security module for RACF has ERROROPT=ABEND specified, then the DB2 subsystem is asked to terminate. If ERROROPT=NOABEND was specified, then the DB2 subsystem is asked to use native DB2 authorization. In either case, the exit is not called again. 

System programmer response: DB2 Version 8 must be executed with the DSNX@XAC that was shipped with DB2 Version 8. The DB2 V8-shipped version must be assembled with the DB2 V8 macros, link edited, and
installed in a library which is accessible to your DB2 subsystem. DB2 Version 7 and DB2 Version 6 must be executed with the IBM DB2 external security module for RACF that was shipped by RACF in ‘SYS1.SAMPLIB(RACF/DB2 external security module)’. This code must be assembled with the DB2 macros of the correct DB2 release, link edited, and installed in a library which is accessible to your DB2 subsystem.

Destination: Descriptor code is 12. Routing codes are 2, 9, and 10.

IRR915I  EXPLRC1 = xxx, EXPLRC2 = xxx, XAPLPRIV = xxxx

Explanation: The IBM DB2 external security module for RACF has been instructed (either by a zap or by changing the assembler source) to display the return and reason code (EXPLRC1 and EXPLRC2) that is returned to DB2 along with the DB2 privilege code (XAPLPRIV) for the request. For DB2 initialization and termination, XAPLPRIV will be xxx

System action: None. This message is a diagnostic informational message.

System programmer response: None. This message is only issued if IBM DB2 external security module for RACF has been specifically altered to display the return, reason, and privilege codes. This should only be done under the guidance of the IBM service team.

Destination: Descriptor code is 4. Routing codes are 9 and 10.

IRR916I  RACF/DB2 EXTERNAL SECURITY MODULE WAS ASSEMBLED WITH AN [HRF7720 OR EARLIER | HRF7730 OR LATER ] MACRO LIBRARY. DB2 ROLES AS RACF CRITERIA ARE [NOT] SUPPORTED.

Explanation: This message is issued when the DB2 V9 RACF access control module is used, to indicate whether the module supports DB2 roles.

The module does not fully support DB2 roles if it is invoked from a DB2 V9 system and any of the following sets of conditions are true:

- The system is running z/OS V1R7 and the RACF access control module was assembled with z/OS V1R7 macros.
- The system is running z/OS V1R7 and the RACF access control module was assembled with z/OS V1R8 macros.
- The system is running z/OS V1R8 and the RACF access control module was assembled with z/OS V1R7 macros.

The module fully supports DB2 roles if it is invoked from a DB2 V9 system and the following set of conditions is true:

- The system is running z/OS V1R8 and the RACF access control module was assembled with z/OS V1R8 macros.

System action: The RACF access control module continues.

System programmer response: Reassemble the RACF access control module with the HRF7730 or later macro library to fully enable ROLES support in the module when DB2 is running on z/OS V1R8 or later. The DB2 V9-shipped version must be assembled with the DB2 V9 macros, link edited, and installed in a library that is accessible to your DB2 subsystem.

Destination: Descriptor code is 4. Routing codes are 9 and 10.
Chapter 6. IRR messages for commands, utilities, and other tasks

This section lists the messages with a prefix of IRR that can go to the user or the system operator. The format of these messages is:

```
IRRxnnnt text
```

where:
- **IRR** identifies the message as a RACF message.
- **xx** identifies the function issuing the message.
- **nnn** is the message serial number.
- **t** is the type code (I = information, or A = action).
- **text** is the text of the message.

The values for the **xx** field that identifies the function issuing the message are:

<table>
<thead>
<tr>
<th>xx</th>
<th>Function or Utility</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>Messages common to several commands</td>
</tr>
<tr>
<td>52</td>
<td>Dynamic parse (IRRDP100 command) messages</td>
</tr>
<tr>
<td>61</td>
<td>RACF cross-reference utility (IRRUT100)</td>
</tr>
<tr>
<td>62</td>
<td>RACF database verification utility (IRRUT200)</td>
</tr>
<tr>
<td>63</td>
<td>Block update command (BLKUPD)</td>
</tr>
<tr>
<td>65</td>
<td>RACF database split/merge utility (IRRUT400)</td>
</tr>
<tr>
<td>67</td>
<td>RACF SMF data unload utility (IRRADU00)</td>
</tr>
<tr>
<td>68</td>
<td>RACF database unload utility (IRRDBU00)</td>
</tr>
<tr>
<td>69</td>
<td>RACF remove ID utility (IRRRID00)</td>
</tr>
<tr>
<td>71</td>
<td>REXX RACVAR function</td>
</tr>
<tr>
<td>A0</td>
<td>RACF subsystem</td>
</tr>
<tr>
<td>B0</td>
<td>RACF subsystem</td>
</tr>
<tr>
<td>C0</td>
<td>RACF subsystem</td>
</tr>
<tr>
<td>D0</td>
<td>DISPLAY command messages</td>
</tr>
<tr>
<td>E0</td>
<td>SIGOFF command messages</td>
</tr>
<tr>
<td>F0</td>
<td>RRSF send request handling task messages</td>
</tr>
<tr>
<td>G0</td>
<td>RRSF parmlib and initialization messages</td>
</tr>
<tr>
<td>H0</td>
<td>SET command messages</td>
</tr>
<tr>
<td>I0</td>
<td>RRSF handshaking messages</td>
</tr>
<tr>
<td>J0</td>
<td>RRSF connection local transaction program messages</td>
</tr>
<tr>
<td>K0</td>
<td>RACLINK command messages</td>
</tr>
<tr>
<td>L0</td>
<td>RACROUTE REQUEST=LIST messages</td>
</tr>
<tr>
<td>L1</td>
<td>CACHECLS profile messages</td>
</tr>
<tr>
<td>M0</td>
<td>TARGET command messages</td>
</tr>
<tr>
<td>N0</td>
<td>RRSF connection receive transaction program messages</td>
</tr>
<tr>
<td>O0</td>
<td>RRSF connection send transaction program messages</td>
</tr>
<tr>
<td>P0</td>
<td>RRSF messages</td>
</tr>
<tr>
<td>Q0</td>
<td>RRSF connection task messages</td>
</tr>
<tr>
<td>R0</td>
<td>RRSF output handling task messages</td>
</tr>
<tr>
<td>S0</td>
<td>RACLINK command messages</td>
</tr>
<tr>
<td>T0</td>
<td>RACLINK command or RRSF output handling task messages</td>
</tr>
<tr>
<td>U0</td>
<td>File allocation messages</td>
</tr>
<tr>
<td>V0</td>
<td>RRSF enveloping messages</td>
</tr>
<tr>
<td>W0</td>
<td>RACPRIV command messages</td>
</tr>
<tr>
<td>X0</td>
<td>RACF operational modes and coupling facility related messages</td>
</tr>
</tbody>
</table>
Messages common to several commands

IRR16001I  command-name failed. profile-name is not a valid profile name for class class-name.

Explanation: The profile name in the indicated command did not follow the format required for profiles in the indicated class.

System action: Command processing stops.

User response: Check the spelling and form of the profile name, and reissue the command.

IRR16003I  WARNING for command-name. The existing internal profile profile-name is not valid and should be deleted.

Explanation: The indicated profile name was found in the database, but it does not follow the format required for profiles in the class related to the indicated command.

System action: In all cases, command processing continues with the next profile name.

User response: Delete the invalid profile with the RDELETE command, or contact your system administrator to delete the profile.

Dynamic parse (IRRDPI00) messages

Dynamic parse messages can be issued at the following times:

- When dynamic parse is initialized
- When IRRDPI00 is run (usually during system IPL)
- When a user issues a RACF command that uses dynamic parse to check the syntax of the operands specified on the RACF command.

IRR52001I  Command IRRDPI00 is invalid when RACF is not active.

Explanation: RACF is not active on the system. RACF must be active to issue the command.

System action: IRRDPI00 command processing stops. No action is taken.

User response: Report this message to your RACF security administrator.

Operator response: Ensure that RACF is available, and IPL the system again.

IRR52002I  User userid not authorized to issue command IRRDPI00.

Explanation: The user indicated in the message is not authorized to issue the IRRDPI00 command.

System action: IRRDPI00 command processing stops. No action is taken.

User response: See your RACF security administrator.


IRR52004I  Command IRRDPI00 failed. Unable to process the parameters specified.

Explanation: IRRDPI00 was unable process the parameters specified.

System action: IRRDPI00 processing stops. No action is taken.

User response: Reissue the IRRDPI00 utility with correct parameters. For a description of IRRDPI00, see z/OS Security Server RACF System Programmer’s Guide.
IRR52005I  Dynamic parse initialization failed. No action was taken. Return code from IKJPARS is return-code

Explanation: A call to the IKJPARS service routine failed with the indicated return code.

System action: IRRDPI00 command processing stops. No action is taken.

User response: Report the exact text of this message to your system programmer.

System programmer response: See “Problem Determination.”

Problem Determination: See z/OS TSO/E Programming Services for an explanation of the return code from the parse service routine.

IRR52006I  Unable to completely parse command command because the command line was incomplete. Processing continues with the next input line.

Explanation: The parse service routine did not receive all the required operands, or an attention interrupt occurred before input was completed.

System action: Processing continues with the next input line in the dynamic parse specifications data set.

User response: Report this message to your system programmer.

System programmer response: Report this message to your IBM support center.

IRR52007I  Command IRRDPI00 failed. No action was taken. Return code from STACK is return-code

Explanation: An error occurred when the STACK service routine attempted to open the SYSUT1 data set.

System action: IRRDPI00 command processing stops. No action is taken.

User response: Report the exact text of this message to your system programmer.

System programmer response: See “Problem Determination.”

Problem Determination: See z/OS TSO/E Programming Services for an explanation of the return code from the PUTLINE service routine.

IRR52008I  Command IRRDPI00 failed. No action was taken. Return code from GETLINE is return-code

Explanation: An error occurred when the GETLINE service routine attempted to read the SYSUT1 data set.

System action: IRRDPI00 command processing stops. No action is taken.

User response: Report the exact text of this message to your system programmer.

System programmer response: See “Problem Determination.”

Problem Determination: See z/OS TSO/E Programming Services for an explanation of the return code from the GETLINE service routine.

IRR52009I  Error in PUTLINE service routine. Processing continues with next input line. Return code is return-code

Explanation: An error occurred when the PUTLINE service routine attempted to echo a line of input.

System action: IRRDPI00 command processing stops. No action is taken.

User response: Report the exact text of this message to your system programmer.

System programmer response: See “Problem Determination.”

Problem Determination: See z/OS TSO/E Programming Services for an explanation of the return code from the PUTLINE service routine.

IRR52010I  Keyword keyword is specified out of order. Processing continues with next command.

Explanation: The dynamic parse specifications commands were specified in the wrong order.

System action: Processing continues with the next input line.

User response: Report this message to your system programmer.

System programmer response: Report this message to your IBM support center.

IRR52011I  Name name is invalid. Possible line continuation problem. Processing continues with next input line.

Explanation: An invalid command was encountered in the input, or, if this is a valid keyword, a continuation character is missing on the previous input line.

System action: Processing continues with the next input line.

User response: Report this message to your system programmer.

System programmer response: Report this message to your IBM support center.
IRR52012I  Segment name invalid for profile type specified. Processing continues with the next command.

**Explanation:** The segment name specified for a PROFILE command is not correct for that profile type.

**System action:** Processing continues with the next DPSDS command set.

**User response:** Report this message to your system programmer.

**System programmer response:** Make sure that the level of the RACF database templates is compatible with the IRRDPSDS data set. Also, make sure that any updates to the templates that affected the IRRDPSDS data set were applied to the database by way of the IRRMIN00 PARM=UPDATE profile and that the system was IPLed to bring the correct templates into storage so the fields and segment names can be verified against those in IRRDPSDS.

IRR52013I  Field name invalid for profile type specified.

**Explanation:** An invalid field name was specified on the KEYWORD command, or a RACF Data Base Template Field definition was not found for the field name specified.

**System action:** Processing continues with the next DPSDS command set.

**User response:** Report this message to your system programmer.

**System programmer response:** Make sure that the level of the RACF database templates is compatible with the IRRDPSDS data set. Also, make sure that any updates to the templates that affected the IRRDPSDS data set were applied to the database by way of the IRRMIN00 PARM=UPDATE profile and that the system was IPLed to bring the correct templates into storage so the fields and segment names can be verified against those in IRRDPSDS.

IRR52014I  SUBFIELD keyword is invalid for flag field specifications. Processing continues with the next command.

**Explanation:** Flag field specifications require only the mask keywords ORMASK and ANDMASK to be specified. Information supplied by the SUBFIELD keyword does not pertain to flag field specifications.

**System action:** Processing continues with the next DPSDS command set.

**User response:** Report this message to your system programmer.

**System programmer response:** Report this message to your IBM support center.

IRR52015I  Mask values are required for flag field specifications, but are not specified. Processing continues with the next command.

**Explanation:** Flag field specifications require the mask keywords ORMASK and ANDMASK to be specified. Information supplied by these commands is used to update the flag field in the RACF database.

**System action:** Processing continues with the next DPSDS command set.

**User response:** Report this message to your system programmer.

**System programmer response:** Report this message to your IBM support center.

IRR52016I  SUBFIELD, TRANSLATE, and ANDMASK/ORMASK are mutually exclusive, only one may be specified. Processing continues with the next command.

**Explanation:** Explicit values are specified by the TRANSLATE keyword; therefore, no variable-value-subfield definition is required (in other words, the SUBFIELD keyword).

**System action:** Processing continues with the next DPSDS command set.

**User response:** Report this message to your system programmer.

**System programmer response:** Report this message to your IBM support center.

IRR52017I  LIST keyword was not specified for a repeat group specification. Processing continues with the next command.

**Explanation:** The LIST keyword was specified and the RACF template definition showed the field named not to be a repeat group field.

**System action:** Processing continues with the next DPSDS command set.

**User response:** Report this message to your system programmer.

**System programmer response:** Report this message to your IBM support center.

IRR52018I  Length of ORMASK is too long for field in RACF database. Processing continues with the next command.

**Explanation:** The value of the mask was too large to fit in the amount of storage available for the field.

**System action:** Processing continues with the next DPSDS command set.
<table>
<thead>
<tr>
<th>IRR Message</th>
<th>Issue Description</th>
<th>System Action</th>
<th>User Response</th>
<th>System Programmer Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRR52019I</td>
<td>Length of ANDMASK is too long for field in RACF data base.</td>
<td>Processing continues with the next command.</td>
<td>Report this message to your system programmer.</td>
<td>Report this message to your IBM support center.</td>
</tr>
<tr>
<td>IRR52020I</td>
<td>Dynamic Parse storage allocation failed. No action taken. Return code is return-code.</td>
<td>Processing stops.</td>
<td>Report this message to your system programmer.</td>
<td>Report this message to your IBM support center.</td>
</tr>
<tr>
<td>IRR52021I</td>
<td>You are not authorized to view segment-name segments.</td>
<td>Processing stops.</td>
<td>Report this message to your system programmer.</td>
<td>Run IRRDPI00 (dynamic parse initialization program). For a description of IRRDPI00, see z/OS Security Server RACF System Programmer’s Guide.</td>
</tr>
<tr>
<td>IRR52022I</td>
<td>Severe program error occurred. Consult your System Programmer. Internal code is code.</td>
<td>Processing stops.</td>
<td>Report the exact text of this message to your system programmer.</td>
<td>Report the exact text of this message to your IBM support center.</td>
</tr>
<tr>
<td>IRR52023I</td>
<td>Invalid input to dynamic parse table update.</td>
<td>No action is taken.</td>
<td>Ensure that the correct dynamic parse specifications data set is specified.</td>
<td></td>
</tr>
<tr>
<td>IRR52024I</td>
<td>Unable to obtain space for Dynamic Parse Update work area. Return code from GETMAIN is return-code.</td>
<td>Dynamic parse issued the GETMAIN macro to obtain space, but the GETMAIN request failed.</td>
<td>If the problem cannot be corrected, report the exact text of this message to your IBM support center.</td>
<td>Run IRRDPI00 (dynamic parse initialization program). For a description of IRRDPI00, see z/OS Security Server RACF System Programmer’s Guide.</td>
</tr>
<tr>
<td>IRR52025I</td>
<td>Unable to obtain space for Dynamic Parse Table. Return code from GETMAIN is return-code.</td>
<td>Dynamic parse issued the GETMAIN macro to obtain space, but the GETMAIN request failed.</td>
<td>If the problem cannot be corrected, report the exact text of this message to your IBM support center.</td>
<td>Run IRRDPI00 (dynamic parse initialization program). For a description of IRRDPI00, see z/OS Security Server RACF System Programmer’s Guide.</td>
</tr>
<tr>
<td>IRR52026I</td>
<td>Unable to FREEMAIN space for dynamic parse table. Size of FREEMAIN is size at location location. Return code is return-code.</td>
<td>Dynamic parse issued the FREEMAIN macro to release space, but the FREEMAIN request failed.</td>
<td>If the problem cannot be corrected, report the exact text of this message to your IBM support center.</td>
<td>Run IRRDPI00 (dynamic parse initialization program). For a description of IRRDPI00, see z/OS Security Server RACF System Programmer’s Guide.</td>
</tr>
</tbody>
</table>
IRR52027I  Unable to perform a check for this field against the RACF template definition because either PROFILE keyword information or SEGMENT keyword information was incomplete. Processing continues with the next command.

Explaination: An error was encountered in the dynamic parse specifications data set.
System action: Processing continues with the next input command.
User response: Report this message to your system programmer.
System programmer response: Report the exact text of this message to your IBM support center.

IRR52028I  Either PROMPT or DEFAULT must be specified for the SUBFIELD keyword. Processing continues with the next input command.

Explaination: An error was encountered in the dynamic parse specifications data set.
System action: Processing continues with the next input command.
User response: Report this message to your system programmer.
System programmer response: Report this message to your IBM support center.

IRR52029I  PROMPT and DEFAULT are mutually exclusive, only one may be specified. Processing continues with the next input command.

Explaination: An error was encountered in the dynamic parse specifications data set.
System action: Processing continues with the next input command.
User response: Report this message to your system programmer.
System programmer response: Report this message to your IBM support center.

IRR52030I  PTYPE must be specified when SUBFIELD is specified.

Explaination: An error was encountered in the dynamic parse specifications data set.
System action: Processing continues with the next input command.

IRR52031I  Command IRRDPI00 failed because the dynamic parse specifications data set is empty. No action was taken.

Explaination: There are no source statements in the dynamic parse specifications data set.
System action: No action was taken.
User response: Report this message to your system programmer.
System programmer response: Ensure the correct dynamic parse specifications data set is specified.

IRR52100I  Processing terminated. Dynamic parse is not active. Contact your system programmer.

Explaination: An operand specified on a RACF command was not recognizable without dynamic parse.
System action: IRRDPI00 command processing stops. No action is taken.
User response: Report this message to your system programmer.
System programmer response: Ensure that IRRDPI00 was run during IPL and that the correct dynamic parse specifications data set was specified. See the z/OS Security Server RACF System Programmer's Guide for more information.

IRR52101I  Processing terminated. Unable to obtain storage for dynamic parse work area.

Explaination: Dynamic parse issued the GETMAIN macro to obtain space, but the GETMAIN request failed.
System action: IRRDPI00 command processing stops. No action is taken.
User response: For TSO users, log on with a larger region size. For batch users, specify a larger region size for the job that failed.
System programmer response: If the problem cannot be corrected, report the exact text of this message to your IBM support center.

IRR52102I  Insufficient storage for internal work area. Processing terminated.

Explaination: Dynamic parse issued the GETMAIN macro to obtain space, but the GETMAIN request failed.
System action: IRRDPI00 command processing stops. No action is taken.

User response: For TSO users, log on with a larger region size. For batch users, specify a larger region size for the job that failed.

System programmer response: If the problem cannot be corrected, report the exact text of this message to your IBM support center.

IRR52103I FREEMAIN failed for PCL work area. Contact your IBM support center.

Explanation: Dynamic parse issued the FREEMAIN macro to release space, but the FREEMAIN request failed.

System action: IRRDPI00 command processing stops. No action is taken.

User response: Report the exact text of this message to your system programmer.

System programmer response: Report the exact text of this message to your IBM support center.

IRR52104I Dynamic parse exit module-name not found in load library. Command processing continues.

Explanation: The RACF dynamic parse exit indicated in the message was not found in the system LNKLST concatenation.

System action: Command processing continues without the function provided by the installation exit.

User response: Report the exact text of this message to your system programmer. Attention: Some exits provide validation of the data you provided, while others may actually change the data from the external format you provided to an internal format suitable for use by the system. Neither the validation nor, if required, the data transformation occurred during execution of this RACF command because the command cannot locate the exit. Therefore, the data you just placed into the segment may contain errors. You should have your system programmer install the needed exit and reissue the command so the exit can examine or modify the data.

System programmer response: Ensure that the indicated exit is in a library in the system LNKLST concatenation.

IRR52105I Field in dynamic parse table is not found in template. Contact your system programmer.

Explanation: A keyword specified in the command is found in the dynamic parse table, but is not found in the associated template.

System action: Command processing stops.

User response: Report this message to your system programmer.

System programmer response: Check that the templates used for the RACF database are correct. If necessary, reinitialize RACF.

IRR52106I Segment not found in Template. Contact your system programmer.

Explanation: A segment name specified on the command is found in the dynamic parse tables, but is not found in the associated templates.

System action: Command processing stops.

User response: Report this message to your system programmer.

System programmer response: Check that the templates used for the RACF database are correct. If necessary, reinitialize RACF.

IRR52107I NOTIFY exit module-name not found.

Explanation: The installation exit indicated in the message was not found.

System action: Command processing continues without the function provided by the installation exit.

User response: Report the exact text of this message to your system programmer.

System programmer response: Ensure that the indicated exit is in a LINKLIB or LPA library.

IRR52108I Insufficient storage for internal workarea. Processing terminated. GETMAIN return code is return-code. Internal code is code.

Explanation: Dynamic parse issued the GETMAIN macro to obtain space, but the GETMAIN request failed.

System action: IRRDPI00 command processing stops. No action is taken.

User response: For TSO users, log on with a larger region size. For batch users, specify a larger region size for the job that failed.

System programmer response: If the problem cannot be corrected, report the exact text of this message to your IBM support center.

IRR52109I Dynamic parse storage allocation failed. No action taken. Return code is return-code.

Explanation: Dynamic parse issued the GETMAIN macro to obtain space, but the GETMAIN request failed.
IRR52110I Insufficient storage for command buffer. Processing terminated.

Explanation: There is not enough storage for the command as issued.

System action: Command processing stops.

User response: For TSO users, log on with a larger region size. For batch users, specify a larger region size for the job that failed.

System programmer response: If the problem cannot be corrected, report the exact text of this message to your IBM support center.

IRR52111I Sub-operands are not allowed with ‘NO-’ keyword. Processing terminated.

Explanation: A sub-operand that begins with NO cannot be specified.

System action: Processing stops.

User response: Report this message to your system programmer.

System programmer response: Report this message to your IBM support center.

IRR52113I Keyword keyword contains invalid or missing subfield(s). Processing continues.

Explanation: One or more subfields specified for the indicated keyword are incorrect or are required.

System action: Processing stops.

User response: Report this message to your system programmer.

System programmer response: Report this message to your IBM support center.

IRR52114I Processing terminated. Unable to obtain storage requested.

Explanation: Dynamic parse issued the GETMAIN macro to obtain space, but the GETMAIN request failed.

System action: IRRDPI00 command Processing stops. No action taken.

User response: For TSO users, log on with a larger region size. For batch users, specify a larger region size for the job that failed.

System programmer response: If the problem cannot be corrected, report the exact text of this message to your IBM support center.

IRR52115I Error during RACF manager processing. Return code is return-code. Reason code is reason-code.

Explanation: A RACF-manager error occurred during request processing.

System action: Command processing stops.

User response: Report the exact text of this message to your system programmer.

Problem Determination: Check the list of RACF-manager return codes in "RACF manager return codes" on page 405. If the return code is listed, the explanation should help you investigate the problem. If the return code is not listed or relates to a problem with RACF (as opposed to a problem you can fix in the RACF database), report the complete text of this message to your IBM support center.

IRR52116I RACF data base access denied — RACF is not currently active or the RACF dataset containing the requested profile is not active.

Explanation: RACF is not active at the time of this request.

System action: No action is taken.

User response: Issue your request again. If the message persists, contact system support.

System programmer response: Check IPL processing to make sure that RACF is activated during system IPL.

IRR52117I LISTING exit module-name not found.

Explanation: The installation exit indicated in the message was not found.

System action: Command processing continues without the function provided by the installation exit.

User response: Report the exact text of this message to your system programmer.

System programmer response: Ensure that the indicated exit is in a LINKLIB or LPA library.

IRR52118I Segment name abbreviation value is ambiguous. Please enter again.

Explanation: The segment name specified is not long enough.

System action: If TSO prompting is on, the user is prompted for a valid segment name abbreviation. If
TSO prompting is off, RACF command Processing stops.

**User response:** Specify a longer segment name abbreviation.

---

**IRR52119I**  
Keyword name abbreviation *value* is ambiguous. Please enter again.

**Explanation:** The keyword name specified is not long enough.

**System action:** If TSO prompting is on, the user is prompted for a valid keyword name abbreviation. If TSO prompting is off, RACF command Processing stops.

**User response:** Specify a longer keyword name abbreviation.

---

**IRR52120I**  
SIZE *size* is out of range.

**Explanation:** The region size specified is incorrect for your system.

**System action:** If TSO prompting is on, the user is prompted for a valid keyword name abbreviation. If TSO prompting is off, RACF command Processing stops.

**User response:** The region size specified is probably too large. If so, specify a smaller region size.

---

**IRR52121I**  
SIZE specified is greater than MAXSIZE. SIZE is adjusted to be equal to MAXSIZE.

**Explanation:** The value specified for SIZE cannot be greater than the value specified for MAXSIZE.

**System action:** RACF adds a user profile, but adjusts SIZE to equal the MAXSIZE operand.

**User response:** To change the SIZE or MAXSIZE operands for this user profile, use the ALTUSER command.

---

**IRR52122I**  
Conflict between SIZE and MAXSIZE. Operand ignored.

**Explanation:** The values specified on the SIZE and MAXSIZE operands are incompatible.

**System action:** RACF adds a user profile, but ignores the SIZE and MAXSIZE operands.

**User response:** To change the SIZE or MAXSIZE operands for this user profile, use the ALTUSER command.

---

**IRR52123I**  
Data must be hexadecimal.

**Explanation:** The data specified can be A through Z or 0 through 9.

**System action:** Command processing stops.

**User response:** Correct the data and issue the command again.

---

**IRR52124I**  
Operand is not valid. Session key interval is not in range 1 - *value*.

**Explanation:** The session key change interval specified for a session segment must be greater than or equal to 1 and less than or equal to *value*, where *value* varies according to the setting of SETROPTS SESSIONINTERVAL. If SETROPTS SESSIONINTERVAL is in effect, or defaulted, then *value* is the SESSIONINTERVAL value. If SETROPTS NOSESSIONINTERVAL is in effect, then the value is 32767.

**System action:** If you are in prompt mode (on TSO, PROFILE PROMPT is in effect), you receive a prompt to reenter the operand. If you are not in prompt mode, command processing stops.

**User response:** Specify a valid value for the INTERVAL operand, by either responding to the prompt, or by reentering the command.

---

**IRR52125I**  
Operand is not valid. Session key exceeds 8 characters.

**Explanation:** The user has entered more than eight characters of character data for a session key. The maximum length is eight characters.

**System action:** If you are in prompt mode (on TSO, PROFILE PROMPT is in effect), you receive a prompt to reenter the operand. If you are not in prompt mode, command processing stops.

**User response:** Specify a valid value for the SESSKEY operand, either by responding to the prompt, or by reentering the command.

---

**IRR52126I**  
RACXTRT failed. Return code is *return-code*. Reason code is *reason-code*.

**Explanation:** RACROUTE REQUEST=EXTRACT failed because of an error in an installation exit, or because of an internal error.

**System action:** Command processing stops.

**User response:** See your RACF administrator.

**Problem Determination:** See the description of return and reason codes for the REQUEST=EXTRACT macro in

[ z/OS Security Server RACROUTE Macro Reference ]

Check any related installation exit for a possible error.
IRR52127I  Field level access checking failed for
        segment segment-name.

Explanation: You do not have authorization to the
        indicated segment.

System action: Command processing stops.

User response: Report the exact text of this message
to your RACF security administrator.

RACF Security Administrator Response: For a
description of field-level access checking, see z/OS
Security Server RACF Security Administrator's Guide

IRR52128I  Mutually exclusive operands are
        specified for keyword keyword.
        Processing terminated.

Explanation: One or more pairs of operands cannot be
        specified together on the indicated keyword in the
        dynamic parse specifications data set.

System action: Processing stops.

User response: Report this message to your system
        programmer.

System programmer response: Report this message to
        your IBM support center.

IRR52129I  The PRIMARY sub-operand was
        ignored. value is not a valid language
        code.

Explanation: The specified PRIMARY sub-operand
        value is not one of the 3-letter codes defined by IBM.

System action: The user's default for the PRIMARY
        language is not changed. Processing continues with the
        next operand or sub-operand. If you issued the
        ADDUSER command and no other messages were
        issued by RACF, the user profile was created.

User response: Issue the ALTUSER command with a
        valid language code specified.

IRR52130I  The PRIMARY sub-operand was
        ignored. The specified language is not
        active.

Explanation: The specified PRIMARY sub-operand
        value is not one of the 3-letter codes defined by IBM.

System action: The user's default for the PRIMARY
        language is not changed. Processing continues with the
        next operand or sub-operand. If you issued the
        ADDUSER command and no other messages were
        issued by RACF, the user profile was created.

User response: Issue the ALTUSER command with a
        valid language code specified.

IRR52131I  The SECONDARY sub-operand was
        ignored. The specified language was not
        active.

Explanation: The specified SECONDARY sub-operand
        value is not one of the 3-letter codes defined by IBM.

System action: The user's default for the SECONDARY
        language is not changed. Processing continues with the
        next operand or sub-operand. If you issued the
        ADDUSER command and no other messages were
        issued by RACF, the user profile was created.

User response: Issue the ALTUSER command with a
        valid language code specified.

IRR52132I  The SECONDARY sub-operand was
        ignored. value is not a valid language
        code.

Explanation: The specified SECONDARY sub-operand
        value is not one of the 3-letter codes defined by IBM.

System action: The user's default for the SECONDARY
        language is not changed. Processing continues with the
        next operand or sub-operand. If you issued the
        ADDUSER command and no other messages were
        issued by RACF, the user profile was created.

User response: Issue the ALTUSER command with a
        valid language code specified.

IRR52133I  The SECONDARY sub-operand was
        ignored. The specified language is not
        active.

Explanation: The specified SECONDARY sub-operand
        value is not one of the 3-letter codes defined by IBM.

System action: The user's default for the SECONDARY
        language is not changed. Processing continues with the
        next operand or sub-operand. If you issued the
        ADDUSER command and no other messages were
        issued by RACF, the user profile was created.

User response: Issue the ALTUSER command with a
        valid language code specified.
value is not one of the 3-letter codes defined by IBM. The specified value was assumed to be an installation-defined language name, but the required language code cannot be obtained from the MVS message service.

**System action:** The user's default for the SECONDARY language is not changed. Processing continues with the next operand or sub-operand. If you issued the ADDUSER command and no other messages were issued by RACF, the user profile was created.

**User response:** Issue the ALTUSER command with a valid language code or language name specified.

---

**IRR52135I**  
The PRIMARY sub-operand was ignored. QRYLANG macro failed with return code xxxx and reason code yyyy.

**Explanation:** The specified PRIMARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was therefore assumed to be an installation-defined language name, but the required language code cannot be obtained because an error condition occurred when the QRYLANG macro of the MVS message service was executing. The return code is indicated by xxxx. The reason code is indicated by yyyy.

**System action:** The user's default for the PRIMARY language is not changed. Processing continues with the next operand or sub-operand. If you issued the ADDUSER command and no other messages were issued by RACF, the user profile was created.

**User response:** Report the complete text of this message to your system programmer.

**System programmer response:** See [z/OS MVS Programming: Authorized Assembler Services Reference LLA-SIU](http://www.ibm.com) for a description of return codes and reason codes for the QRYLANG macro.

---

**IRR52136I**  
The SECONDARY sub-operand was ignored. QRYLANG macro failed with return code xxxx and reason code yyyy.

**Explanation:** The specified SECONDARY sub-operand value is not one of the 3-letter codes defined by IBM. The specified value was therefore assumed to be an installation-defined language name, but the required language code cannot be obtained because an error condition occurred when the QRYLANG macro of the MVS message service was executing. The return code is indicated by xxxx. The reason code is indicated by yyyy.

**System action:** The user's default for the SECONDARY language is not changed. Processing continues with the next operand or sub-operand. If you issued the ADDUSER command and no other messages were issued by RACF, the user profile was created.

**User response:** Report the complete text of this message to your system programmer.

**System programmer response:** See [z/OS MVS Programming: Authorized Assembler Services Reference LLA-SIU](http://www.ibm.com) for a description of return codes and reason codes for the QRYLANG macro.

---

**IRR52137I**  
Purge of VLF class IRRUMAP failed with return code nn.

**Explanation:** Dynamic parse attempted to purge a VLF entry in the UID-to-user ID mapping table because a change was made to UID information by an ALTUSER or DELUSER command. The module called to purge the entry, IRRMAP00, returned an unexpected return code.

**System action:** Command processing successfully updates the user profile, but the in-storage information that maps the user ID to a UID may not match the information on the RACF database.

**User response:** Report the exact text of this message to your system programmer.

**System programmer response:** Report the exact text of this message to your IBM support center. The following decimal return codes may appear in the message. They indicate an unexpected error in the command’s processing or the user's TSO environment:

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Object not found in VLF</td>
</tr>
<tr>
<td>12</td>
<td>No ACEE available</td>
</tr>
<tr>
<td>16</td>
<td>VLF failure</td>
</tr>
<tr>
<td>20</td>
<td>ACEE is not version 2</td>
</tr>
<tr>
<td>999</td>
<td>Parameter list error</td>
</tr>
</tbody>
</table>

---

**IRR52138I**  
Purge of VLF class IRRGMAP failed with return code nn.

**Explanation:** Dynamic parse attempted to purge a VLF entry in the GID-to-group name table because a change was made to GID information by an ALTGROUP or DELGROUP command. The module called to purge the entry, IRRMAP00, returned an unexpected return code.

**System action:** Command processing successfully updates the group profile, but the in-storage information that maps the group name to a GID may not match the information on the RACF database.

**User response:** Report the exact text of this message to your system programmer.

**System programmer response:** Report the exact text of this message to your IBM support center. The following decimal return codes may appear in the message. They indicate an unexpected error in the command’s processing or the user's TSO environment:

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Object not found in VLF</td>
</tr>
<tr>
<td>12</td>
<td>No ACEE available</td>
</tr>
<tr>
<td>16</td>
<td>VLF failure</td>
</tr>
<tr>
<td>20</td>
<td>ACEE is not version 2</td>
</tr>
<tr>
<td>999</td>
<td>Parameter list error</td>
</tr>
</tbody>
</table>
IRR52139I  KEYMASKED or KEYENCRYPTED data must be 16 hexadecimal characters.

Explanation: You entered data in the KEYMASKED or KEYENCRYPTED suboperand that:
- Is not exactly 16 characters long.
- Contains characters other than the hexadecimal characters 0 through 9 and A through F.

System action: If TSO prompting is active for the session, TSO prompts you to re-enter the suboperand. If TSO prompting is not active, command processing stops.

User response: Reenter the suboperand correctly. Be sure it is 16 characters long and contains only characters 0 through 9 and A through F.

IRR52140I Either the KEYMASKED or the KEYENCRYPTED sub-operand has been specified twice. Command Processing stops.

Explanation: You entered the KEYMASKED or KEYENCRYPTED suboperand twice. The suboperand can be specified only once.

System action: Command processing stops.

User response: Reenter the command and specify the KEYMASKED or KEYENCRYPTED suboperand only once.

IRR52141I KEYMASKED and KEYENCRYPTED are mutually exclusive sub-operands, and both have been specified. Command Processing stops.

Explanation: You specified both the KEYMASKED and the KEYENCRYPTED suboperands, which are mutually exclusive. You can specify only one operand at a time.

System action: Command processing stops.

User response: Reenter the command with either the KEYMASKED or the KEYENCRYPTED suboperand.

IRR52142I The KEYENCRYPTED sub-operand was specified but a Cryptographic product is not available on this system. Command Processing stops.

Explanation: The KEYENCRYPTED suboperand is not available. A cryptographic product is not available on this system.

System action: Command processing stops.

User response: Reenter the command with the
Chapter 6. IRR messages for commands, utilities, and other tasks 197
IRR52151I

Unexpected RACROUTE REQUEST=EXTRACT error while retrieving profile profile. SAF RC = safrc, RACF RC = racfc, RACF RSN = rsncode.

Explanation: This message gives the resulting SAF return code, a RACF return code (SAFPRRET), and a RACF reason code (SAFPRREA). If the value of a return code or reason code is greater than X'0000FFFF', it is displayed as a hexadecimal number. If the value is less than or equal to X'0000FFFF', it is displayed as a decimal number.

This message can be issued in the following situations:

- If the message indicates a USER, GROUP, CONNECT, or STARTED profile, the message is issued when an RDEFINE or RALTER command specifies the STDATA segment. An unexpected error occurred from a RACROUTE REQUEST=EXTRACT macro that was used to retrieve information for the STDATA segment.
- If you modified DCE, OMVS, or OVM information in a user profile, the DCE, OMVS, or the OVM segment of the RACF profile changed but the corresponding update in the DCEUUIDS, UNIXMAP, or VMPOSIX class for the user or group profile did not occur. RACF attempted to retrieve the information from the profile specified in the message text but has encountered an error.
- If you modified LNOTES, NDS, or KERB information in a USER profile, the LNOTES, NDS, or KERB segment of the profile changed but the corresponding NOTELINK, NDSLINK, or KERBLINK mapping class profile was not updated. RACF attempted to retrieve the LNOTES, NDS, or KERB information from the profile specified in the message text but has encountered an error.
- If the message indicates a profile in the CDT class, the message is issued when an RDEFINE or RALTER command specifies the CDTINFO segment. An unexpected error occurred from a RACROUTE REQUEST=EXTRACT macro that was used to retrieve information for the CDTINFO segment; some validation checking on the fields in the CDTINFO segment, therefore, cannot be completed.

System action: Command processing continues in a specific way for each of the following situations:

- If the message indicates a USER, GROUP, CONNECT, or STARTED profile, processing of the RDEFINE or RALTER command completed successfully. Data specified for the STDATA segment was processed, along with any other data on the command.
- If you were modifying DCE, OMVS, or OVM information in a user profile, command processing continues. However, the mapping profiles in the DCEUUIDS, UNIXMAP, or VMPOSIX class are not updated.
- If you were modifying LNOTES, NDS, or KERB information in a user profile, command processing continues. However, the mapping profiles in the NOTELINK, NDSLINK, or KERBLINK class are not updated.
- If the message indicates a profile in the CDT class, processing of the RDEFINE or RALTER command completed successfully. Data specified for the CDTINFO segment was processed, along with any other data on the command. The data in the CDTINFO segment, however, may contain errors.

User response: Report this message to the system programmer and provide the exact text of the command you issued.

System programmer response: Use the return code information in z/OS Security Server RACROUTE Macro Reference to determine the error condition and fix the error. If necessary, contact the IBM support center. Tell them the command issued and the resulting return and reason codes.

- If you were updating DCE, OMVS, or OVM information and you have corrected the error, reissue the command. As an alternative, use the RACF RALTER or RDELETE command to manually administer the DCEUUIDS, UNIXMAP, or VMPOSIX class profile that corresponds to the user profile you were changing.
- If you were updating OMVS or OVM information in user or group profiles, you can use the RACF RDEFINE or PERMIT command to manually update the access list of the appropriate UNIXMAP or VMPOSIX class profile.
- If you were updating LNOTES, NDS, or KERB information and you have corrected the error, reissue the command. As an alternative, try to delete the information and add it again. If the SNAME, UNAME, or KERBNAME values are in upper case characters, use the RACF RALTER or RDELETE command to manually administer the NOTELINK, NDSLINK, or KERBLINK class profile that corresponds to the user profile you were changing.

For details on the mapping profiles, see z/OS Security Server RACF Security Administrator's Guide.

- If you were adding or updating a profile in the CDT class and you have corrected the error, issue the RALTER command with the CDTINFO keyword and no suboperands:
  RALTER CDT profile CDTINFO

This will initiate validation checking of fields within the CDTINFO segment. You may also issue the RLIST command to examine the contents of the CDTINFO segment in the profile to ensure the field contents are correct.
IRR52152I Both AT and ONLYAT cannot be specified for the same command. The command is not issued.

Explanation: The AT and ONLYAT keywords are mutually exclusive. Only one may be specified.

System action: Command processing ends.

User response: Issue the command again, specifying either the AT or ONLYAT keyword, but not both.

IRR52153I Unexpected return code return-code and reason code reason-code encountered while attempting an ICHEINTY operation.

Explanation: An ICHEINTY macro was issued to update the RACF database but returned an unexpected return and reason code. The error occurred when RACF attempted to update one of the following:

- A UUID-to-user ID mapping profile because an ADDUSER, ALTUSER, or DELUSER command changed the DCE UUID information.
- A UNIXMAP class mapping profile because an ADDUSER, ALTUSER, DELUSER, ADDGROUP, ALTGROUP, or DELGROUP command changed an OMVS UID or OMVS GID
- A VMPOSIX class mapping profile because an ADDUSER, ALTUSER, DELUSER, ADDGROUP, ALTGROUP, or DELGROUP command changed an OVM UID or OVM GID
- A NOTELINK, NDSLINK, or KERBLINK mapping profile because an ADDUSER, ALTUSER, or DELUSER command changed an LNOTES SNAME, an NDS UNAME, or KERB KERBNAME.

Return code return-code and reason code reason-code are displayed in decimal. Message IRR52154I follows this message immediately and identifies the mapping profile that was being changed.

System action: The profile is updated according to each of the following circumstances:

- If you are modifying DCE UUIDs contained in RACF user profiles, command processing updates the user profile successfully. However, the mapping profile in the DCEUUIDS class that maps the DCEUUID to a RACF user ID might not match the information in the user profile.
- If you are modifying OMVS information in user or group profiles (UID or GID), command processing updates the profile successfully. However, the mapping profile in the UNIXMAP class that maps an OMVS UID or OMVS GID to a RACF user or group might not match the information in the corresponding profile.
- If you are modifying OVM information in user or group profiles (UID or GID), command processing updates the profile successfully. However, the mapping profile in the VMPOSIX class that maps a POSIX UID or POSIX GID to a RACF user or group might not match the information in the corresponding profile.
- If you are modifying LNOTES or NDS information in a user profile (SNAME or UNAME), command processing updates the profile successfully. However, the mapping profile in the NOTELINK or NDSLINK class that maps an LNOTES SNAME or NDS UNAME to a RACF user might not match the information in the corresponding profile. See message IRR52154I for information describing the mismatch.

System programmer response: If the problem occurred with the NOTELINK, NDSLINK, or KERBLINK profiles, see message IRR52154I for the steps you need to follow to correct the error.

Report the exact text of this message to the IBM support center. For details on the mapping profiles, see z/OS Security Server RACF Security Administrator’s Guide.

User response: Report the exact text of this message to your system programmer.

IRR52154I The information in the class1 mapping profile profile1 does not match the profile2 profile in the class2 class.

Explanation: This message, which follows IRR52153I, identifies the mapping profile that was being changed when the error described in IRR52153I occurred. See that message for further information.

System action: The user or group profile specified in the RACF command was updated successfully. However, the DCEUUIDS, NOTELINK, NDSLINK, VMPOSIX, or KERBLINK mapping profiles were not updated. See IRR52153I for a detailed explanation.

System programmer response: If the problem occurred with the NOTELINK, NDSLINK, or KERBLINK profiles, perform the following steps:

1. Determine the first user ID that was assigned this application user name.
   - If the application user name contains lower case letters, use the RLIST NOTELINK *, RLIST NDSLINK *, or RLIST KERBLINK * command in the background to display the user ID in the Application Data field of the resource profile for the NOTELINK, NDSLINK, or KERBLINK class.
   - If the application user name contains only upper case letters, issue the RLIST NOTELINK profile-name, RLIST NDSLINK profile-name, or RLIST KERBLINK profile-name command, using the terminal monitoring program (TMP). You can find the user ID in the application data field.

2. If the Application Data field contains the user ID that should be associated with this LNOTES SNAME, NDS UNAME, or KERB KERBNAME,
I RR52155I • IRR52159I

then no further problem determination or corrective actions are necessary. The IRR52153I message indicates that a residual NOTELINK, NDSLINK, or KERBLINK profile was found. However, the information in the profile is correct.

3. If the Application Data field does not contain the user ID that should be associated with this LNOTES SNAME, NDS UNAME, or KERB KERBNAME, then issue an ALTUSER command with the NOLNOTES, NONDS, or NOKERB operand for that user ID.

4. Select a new LNOTES SNAME, NDS UNAME, or KERB KERBNAME for this user ID and issue a new ALTUSER command to associate this user ID with the new SNAME, UNAME, or KERBNAME.

5. Issue the ALTUSER command again for the original user ID and specify the user's original SNAME, UNAME, or KERBNAME. This recreates the original user's identity mapping profile that was deleted in step 3.

If the problem occurred with any of the other mapping profiles, report the exact text of this message to the IBM support center. For details on the mapping profiles, see z/OS Security Server RACF Security Administrator's Guide.

IRR52155I The DCE principal UUID must be unique for each RACF User ID. The DCEUUUIDS mapping profile is not updated.

Explanation: RACF has detected that an ADDUSER or ALTUSER command tried to assign a principal UUID to more than one RACF user. Although the ADDUSER or ALTUSER command can complete successfully, a corresponding update is not made in the DCEUUUIDS class.

System action: The DCE segments of the user profiles specified on the command line are updated. However, the appropriate DCEUUUIDS class profile for each user does not change.

User response: Determine the correct principal UUID as listed in the DCE registry for this RACF/DCE user. Reissue the ALTUSER command to set the principal UUID in the RACF DCE segment to the UUID listed in the DCE registry.

IRR52156I Purge of VLF class IRRSMAP failed with return code return-code.

Explanation: RACF attempted to purge a VLF entry in the user ID-to-USP mapping table because z/OS UNIX System Services information was changed by an ALTUSER, DELUSER, or ALTGROUP command. The module called to purge the entry, IRRMAP00, returned an unexpected return code.

System action: Command processing successfully updates the user or group profile, but the in-storage information that maps a user ID to a USP may not match the information in the RACF database.

User response: Report the exact text of this message to your system programmer.

System programmer response: Report the exact text of this message to the IBM support center. The following decimal return codes may appear in the message. They indicate an error in the command’s processing or the user’s TSO environment:

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Object not found in VLF</td>
</tr>
<tr>
<td>12</td>
<td>No ACEE available</td>
</tr>
<tr>
<td>16</td>
<td>VLF failure</td>
</tr>
<tr>
<td>20</td>
<td>ACEE is not version 2</td>
</tr>
<tr>
<td>999</td>
<td>Parameter list error</td>
</tr>
</tbody>
</table>

IRR52157I Field field-name is not allowed for a profile in class class-name.

Explanation: An attempt was made to define a field that is not allowed for a profile in the indicated class.

System action: Command processing ends.

User response: Decide whether the field name or class name was in error and issue a corrected command if necessary.

System programmer response: If the failing command was generated by an application, contact the service personnel responsible for that application.

IRR52158I Field field-name exceeds limit characters.

Explanation: The value specified for the field is too long. The maximum length is limit.

System action: Command processing ends.

User response: Retry the command specifying a shorter field value.

System programmer response: If the failing command was generated by an application, contact the service personnel responsible for that application.

IRR52159I Required subfield subfield-name in field field is not specified.

Explanation: A required subfield of a field specification is missing.

System action: Command processing ends.

User response: Include the indicated subfield and retry the command.

System programmer response: If the failing command was generated by an application, contact the service personnel responsible for that application.
IRR52160I  Subfield subfield-name in field field is not valid.

Explanation:  An incorrect value was identified for the indicated subfield.

- For conditional access authority, the value must be NONE, EXECUTE, READ, UPDATE, CONTROL, or ALTER.
- For a conditional access class, the value must be APPCPORT, CONSOLE, JESINPUT, PROGRAM, TERMINAL, or SYSID.

System action:  Command processing ends.

User response:  Retry the command specifying a valid value for the subfield.

System programmer response:  If the failing command was generated by an application, contact the service personnel responsible for that application.

IRR52161I  The application user identity must be unique for each RACF User ID. The mapping profile for userid will not be updated.

Explanation:  An ADDUSER or ALTUSER command tried to assign the same Lotus Notes® for z/OS short name or Novell Directory Services user name to more than one RACF user. Although the command can complete successfully, a corresponding update is not made in the corresponding NOTELINK or NDSLINK mapping class.

System action:  The LNOTES or NDS segment of the user profile specified by the command is updated. However, the appropriate NOTELINK or NDSLINK class profile for each user does not change.

User response:  To correct the problem, perform the following steps:
- Determine the first user ID that was assigned this application user name.
  - If the application user name contains lower case letters, use the RLIST NOTELINK * or RLIST NDSLINK * command in the background to display the user ID in the application data field of the resource profile for the NOTELINK or NDSLINK class.
  - If the application user name contains only upper case letters, issue the RLIST NOTELINK profile-name or RLIST NDSLINK profile-name command, using the terminal monitoring program (TMP). You can find the user ID in the application data field.
- Issue an ALTUSER command with the NOLNOTES or NONDS operand for that user ID.
- Select a new short name for user userid and issue a new ALTUSER command to associate this user ID with a new short name or user name.

4. Issue the ALTUSER command again for the original user ID and specify the user's original short name or user name. This recreates the original user's identity mapping profile that was deleted in step 2.

IRR52162I  Unable to determine the name of the local Kerberos realm. Command processing ends.

Explanation:  An ADDUSER KERB (KERBNAME) or ALTUSER KERB (KERBNAME) command was issued, but the local Kerberos realm is not defined to RACF. The local Kerberos realm must be defined to RACF before a local Kerberos principal name can be defined.

System action:  Command processing ends.

User response:  If the KERBDFLT REALM class profile is not defined, use RDEFINE to define the KERBDFLT profile in the REALM class and supply the KERBNAME operand to define the name of the local Kerberos realm. If the KERBDFLT REALM class profile is already defined, specify the KERBNAME operand on a RALTER command to define the name of the local Kerberos realm.

System programmer response:  If the failing command was generated by an application, contact the service personnel responsible for that application.

IRR52163I  The "char" character is not allowed in KERBNAME. Command processing ends.

Explanation:  The name specified using the KERBNAME operand contains the character "char", which is not allowed. A local Kerberos principal name (defined by the ADDUSER or ALTUSER command) must not include the "@" character; a local Kerberos realm name (defined by the RDEFINE or RALTER command) must not contain the "/" character.

System action:  Command processing ends.

User response:  Reissue the command specifying a valid KERBNAME.

System programmer response:  If the failing command was generated by an application, contact the service personnel responsible for that application.

IRR52164I  KERBNAME may not be prefixed by "/.../". Command processing ends.

Explanation:  RACF uses a convention of "/.../realm_name/principal_name" to represent fully qualified Kerberos foreign principal names. Local Kerberos principal names, however, may not be fully qualified when specified on an ADDUSER or ALTUSER command. A KERBNAME that begins with the string "/.../" would be interpreted as a fully qualified name, so the prefix is not allowed.

System action:  Command processing ends.

User response:  Reissue the command specifying a valid KERBNAME.

System programmer response:  If the failing command was generated by an application, contact the service personnel responsible for that application.

Chapter 6. IRR messages for commands, utilities, and other tasks  201
IRR52165I  The value for the segment_name segment operand_name operand must be unique. Command processing ends.

Explanation: The application identity name assigned for the segment_name segment by the ADDUSER or ALTUSER command is already assigned to another RACF user. The same application identity name cannot be assigned to more than one user. If a list of users had been specified in the command, the command fails because the same application identity name would have been assigned to each user in the list.

System action: Command processing ends.

User response: Reissue the command, specifying a unique name in the operand_name operand.

IRR52166I  The fully qualified form of the local Kerberos principal name must not exceed 240 characters. Command processing ends.

Explanation: The length of the fully qualified form of the local Kerberos principal name (/.../local_realm_name/local_principal_name) exceeds the limit of 240 characters.

System action: Command processing ends.

User response: Use the RLIST command to determine the name of the local Kerberos realm, then reissue the ADDUSER or ALTUSER command, specifying a local Kerberos principal name that will not exceed the 240 character limit in its fully qualified form.

IRR52167I  Unable to validate MINTKTLFE, MAXTKTLFE, and DEFTKTLFE. Ticket lifetime values are ignored.

Explanation: Specified values for ticket lifetime (MINTKTLFE, MAXTKTLFE, or DEFTKTLFE) cannot be validated and will be ignored. Validation requires all three ticket lifetime values. However, one or more ticket lifetime values cannot be determined.

System action: Ticket lifetime values are ignored.

User response: Determine which ticket lifetime values are required and reissue the command using the following guidelines:

- For the RDEFINE command, all three ticket lifetime values (MINTKTLFE, MAXTKTLFE, and DEFTKTLFE) must be specified together on the same command.
- For the RALTER command, if the ticket lifetime values are being initially defined, all three values (MINTKTLFE, MAXTKTLFE, and DEFTKTLFE) must be specified together on the same command.
- For the RALTER command, if previously defined ticket lifetime values are being changed, any undefined values (MINTKTLFE, MAXTKTLFE, or DEFTKTLFE) must be specified together on the same command.

If ticket lifetime values have been previously defined for this local Kerberos realm, the RALTER command may be used to alter one or more of them, but if any one of them has been deleted by means of the NOMINTKTLFE, NOMAXTKTLFE, or NODEFTKTLFE operand, this ticket lifetime value is no longer defined and must be included on the same RALTER command. Use the RLIST command to determine undefined values.

IRR52168I  Values specified for MINTKTLFE, MAXTKTLFE, or DEFTKTLFE are not valid. Ticket lifetime values are ignored.

Explanation: The ticket lifetime values are not consistent with each other. The value of MINTKTLFE must be less than the value of MAXTKTLFE and the value of DEFTKTLFE must be greater than the value of MINTKTLFE and less than the value of MAXTKTLFE.

System action: Ticket lifetime values are ignored.

User response: Use the RLIST command to determine the current ticket lifetime values, if any. Reissue the command, specifying valid values for MINTKTLFE, MAXTKTLFE, or DEFTKTLFE.

IRR52169I  A request to process Kerberos key information for profile-name failed. Command processing continues.

Explanation: An error occurred while attempting to generate a Kerberos key for the user or REALM class profile that is having its password changed through the use of the ALTUSER, RDEFINE, or RALTER command.

System action: All processing except for the key update is completed.

User response: Use the RLIST command to list the KERBDFLT profile definition of the local Kerberos realm in the REALM class and verify that the local realm name (KERBNAME) is defined. Use the appropriate list command (LISTUSER, RLIST) to list the KERB segment information for this user or REALM class and verify that this information may be accessed. Correct any problems and reissue the command.

IRR52170I  The LDAP URL specified by the LDAPHOST operand was not prefixed by "ldap://" or "ldaps://". Command processing ends.

Explanation: An LDAP URL must start with either ldap:// or ldaps://, such as ldap://123.45.6:389 or ldaps://123.45.6:636.

System action: Command processing ends.

User response: Reissue the command, specifying an
LDAP URL with the appropriate ldap:// or ldaps:// prefix.

**IRR52171I**  
**Password not valid for LDAP BIND.**  
**Command processing ends.**

**Explanation:** The specified password is not valid for LDAP BIND. For example, it should not start with the '{' character (hexadecimal x'8B').

**System action:** Command processing ends.

**User response:** Reissue the command, specifying a password that is valid for LDAP BIND.

---

**IRR52172I**  
**A request to process LDAP BIND password information for profile-name failed. Command processing continues.**

**Explanation:** An error occurred while attempting to mask or encrypt the LDAP BIND password that was specified for the user or FACILITY class profile PROXY segment through the use of the ADDUSER, ALTUSER, RDEFINE, or RALTER command.

**System action:** All processing except for the LDAP BIND password update is complete. The LDAP BIND password has not been added to the user or FACILITY class profile PROXY segment.

**User response:** Use the SETROPTS command to determine if the KEYSMSTR class is activated. Use the RLIST command to determine that the KEYSMSTR class LDAP.BINDPW.KEY profile has been defined and that it has a SSIGNON segment that contains either a masked or encrypted key. If key encryption is requested, determine that a cryptographic product is present on the system and that it is active. The cryptographic product must be active when you define the profile to the KEYSMSTR class. Correct any problems and reissue the command.

---

**IRR52173I**  
**RACF was unable to determine if additional application password processing is required. Command processing continues.**

**Explanation:** A TSO parse error prevented RACF from determining if the command contains an application password that requires additional processing, such as:

- Generation of a Kerberos key
- Encryption or masking of an LDAP BIND password

**System action:** All processing except for the additional application password processing is completed.

- If the command specified a password that should be used to generate a Kerberos key, the key was not generated and not stored in the RACF profile.
- If the command specified an LDAP BIND password, the password was not encrypted or masked and not stored in the RACF profile.

**User response:** Do one of the following tasks:

1. Choose another value for id and issue SEARCH CLASS(USER) UID(id) or SEARCH CLASS(GROUP) GID(id) to make sure the new value is not also in use. Then, reissue the original command with the new value for id.
2. Let RACF choose an unused value for you by reissuing the command with the AUTOUID or AUTOGID keyword. For example: ADDUSER JORDAN OMVS(AUTOUID)
3. Reissue the command with the SHARED keyword to force RACF to assign the id despite it already being in use. The SHARED keyword requires the SPECIAL attribute or READ authority to the SHARED.IDS resource in the UNIXPRIV class.

**IRR52174I**  
**Incorrect [UID|GID] id. This value is already in use by name.**

**Explanation:** You tried to assign a user a UID value that is already in use, or you tried to assign a group a GID that is already in use. The user or group is identified by name. Note that it is possible that more than one user or group is currently using the value, but only one of them is identified, and that one is arbitrarily chosen. If you want to see a complete list, issue SEARCH CLASS(USER) UID(id) or SEARCH CLASS(GROUP) GID(id).

**System action:** Command processing stops.

**RACF Security Administrator Response:** If the command issuer should be allowed to assign shared UIDs and GIDs, then permit the user with READ access to the resource named SHARED.IDS in the UNIXPRIV class. The user should then reissue the command using the SHARED keyword.

**User response:** Do one of the following tasks:

1. Choose another value for id and issue SEARCH CLASS(USER) UID(id) or SEARCH CLASS(GROUP) GID(id) to make sure the new value is not also in use. Then, reissue the original command with the new value for id.
2. Let RACF choose an unused value for you by reissuing the command with the AUTOUID or AUTOGID keyword. For example: ADDUSER JORDAN OMVS(AUTOUID)
3. Reissue the command with the SHARED keyword to force RACF to assign the id despite it already being in use. The SHARED keyword requires the SPECIAL attribute or READ authority to the SHARED.IDS resource in the UNIXPRIV class.

**IRR52175I**  
**You are not authorized to specify the SHARED keyword.**

**Explanation:** You are attempting to specify the SHARED keyword to assign a UID or GID value that is already in use. You have not been authorized for this action.

**System action:** Command processing stops.

**RACF Security Administrator Response:** If appropriate, permit the user with READ access to the SHARED.IDS profile in the UNIXPRIV class, and refresh the UNIXPRIV class. Then have the user reissue the command.
**User response:** Contact your security administrator.

**Explanation:** You are attempting to assign a UID or GID in the OMVS segment, and the security administrator has indicated that shared UIDs and GIDs should be controlled. However, control of shared UIDs and GIDs requires the RACF database to be at least at stage 2 of application identity mapping, and this is not the case.

**System action:** Command processing stops.

**System programmer response:** Use the IRRIRA00 utility to convert the RACF database to at least stage 2 of application identity mapping. See the z/OS Security Server RACF System Programmer's Guide for information about the IRRIRA00 utility. Once this is complete, the user may reissue the command.

**RACF Security Administrator Response:** Either remove the SHARED.IDS profile from the UNIXPRIV class, or contact the system programmer and have him implement application identity mapping.

**User response:** Contact your security administrator or system programmer.

---

**IRR52177I** [User | Group] name was assigned an OMVS [UID | GID] value of id.

**Explanation:** In response to your request, a unique value, id, has been generated by RACF for the UID of user name or for the GID of group name in the OMVS segment. If a unique UID or GID value already existed in the OMVS segment of this USER or GROUP profile, then it is unchanged, and its value is what is displayed in this message. If a unique UID or GID value already existed, and RACF Remote Sharing Facility (RRSF) automatic command direction is in effect for the USER or GROUP class, then the command will be propagated with the OMVS UID or GID keyword specifying the preexisting value.

**User response:** Contact your security administrator.

---

**IRR52178I** You cannot use automatic [UID | GID] assignment when a value already exists.

**Explanation:** You asked RACF to generate a unique value for either a UID or GID in the OMVS segment, however, a (non-unique) value already exists.

**User response:** Contact your security administrator.

---

**IRR52181I** The BPX.NEXT.USER profile has run out of possible [UID | GID] values.

**Explanation:** In the course of automatically assigning UID or GID values, the maximum eligible value has been reached. RACF determines eligible UID and GID values by using the APPLDATA information of the BPX.NEXT.USER profile in the FACILITY class. If a...
single UID or GID value had been defined as a starting point, the maximum value of 2,147,483,647 has been reached. If a range of available UID or GID values had been defined, the upper bound of that range has been reached.

System action: Command processing stops.

RACF Security Administrator Response: Change the APPLDATA of the FACILITY class profile named BPX.NEXT.USER to specify an alternate starting point or range. If RRSF is active, make sure the value you specify does not overlap with criteria specified in BPX.NEXT.USER on other RRSF nodes, or UID/GID collisions can occur across your network. If you are using automatic command propagation for the FACILITY class, make sure you use the ONLYAT keyword on the RALTER command when updating BPX.NEXT.USER or else your update will be propagated to the BPX.NEXT.USER profile on the other nodes.

User response: Contact your security administrator.

IRR52182I Automatic [UID | GID] assignment requires application identity mapping to be implemented.

Explanation: The AUTOUID or AUTOGID keyword has been specified, but the RACF database has not been converted to the use of application identity mapping. Application identity mapping must be enabled in order for RACF to guarantee that the assigned UID or GID is unique. Use of the UNIXMAP class is not sufficient. The RACF database must be at least at stage 2 of application identity mapping.

System action: Command processing stops.

System programmer response: Use the IRRIRA00 utility to convert the RACF database to at least stage 2 of application identity mapping. See the z/OS Security Server RACF System Programmer’s Guide for information about the IRRIRA00 utility. Once this is complete, the user may reissue the command.

User response: Contact your system programmer.

IRR52183I Use of automatic [UID | GID] assignment requires SHARED.IDS to be implemented.

Explanation: The AUTOUID or AUTOGID keyword has been specified, but shared UID/GID control has not been implemented. Shared UID/GID control must be implemented in order for RACF to guarantee that the assigned UID or GID is unique.

System action: Command processing stops.

RACF Security Administrator Response: You must implement the SHARED.IDS profile in the UNIXPRIV class in order to activate shared UID/GID control, which is a prerequisite for the automatic UID/GID function. See the z/OS Security Server RACF Security Administrator’s Guide for details on shared UID/GID control. Once this is complete, the user may reissue the command.

User response: Contact your security administrator.

IRR52184I You cannot use automatic [UID | GID] assignment with a list of names.

Explanation: You asked RACF to generate a unique value for either a UID or GID in the OMVS segment, but you specified a list of names on the command. Automatic id generation does not support this command syntax.

System action: Command processing stops.

User response: If you want RACF to assign a UID or GID value for each name, issue a separate command for each name.

IRR52185I The same [UID | GID] cannot be assigned to more than one [user | group].

Explanation: You tried to assign a UID to a list of users, or a GID to a list of groups, but shared UNIX ids are not allowed.

System action: Command processing stops.

User response: Issue a separate command with a different value for each name. If the names really require the same id, then reissue the command specifying the SHARED keyword. The SHARED keyword requires the SPECIAL attribute or READ authority to the SHARED.IDS resource in the UNIXPRIV class.

IRR52186I You cannot specify both [AUTOUID | AUTOGID] and SHARED.

Explanation: You specified either the AUTOUID or AUTOGID keyword and the SHARED keyword, but they are mutually exclusive.

System action: Command processing stops.

User response: Correct and reissue the command.

IRR52187I Incorrect APPLDATA syntax for the BPX.NEXT.USER profile.

Explanation: You have used the AUTOUID or AUTOGID keyword to request an automatically generated UID or GID. RACF derives the next available value using criteria specified in the APPLDATA field of the BPX.NEXT.USER profile in the FACILITY class. However, the APPLDATA contains a syntactically incorrect string.

System action: Command processing stops.

RACF Security Administrator Response: Correct the APPLDATA. The format of the APPLDATA is a valid
UID value, or range of UID values, followed by a forward slash, followed by a valid GID value, or range of GID values. See the `z/OS Security Server RACF Security Administrator’s Guide` for details on defining BPX.NEXT.USER.

If RRSF is active, make sure the value you specify does not overlap with criteria specified in BPX.NEXT.USER on other RRSF nodes, or UID/GID collisions can occur across your network. If you are using automatic command propagation for the FACILITY class, make sure you use the ONLYAT keyword on the RALTER command when updating BPX.NEXT.USER or else your update will be propagated to the BPX.NEXT.USER profile on the other nodes.

User response: Contact your security administrator.

**IRR52188I**  
The POSIT value is missing for the CDT profile **profile-name**. You must correct this error before the class **profile-name** can be added to the dynamic class descriptor table.

Explanation: A profile was defined in the CDT class, but the CDTINFO(POSIT(nnn)) keyword was omitted. The POSIT value is required before the dynamic class descriptor table is built or rebuilt.

System action: Command processing continues, and the CDT profile is placed in the RACF database. If the SETROPTS RACLST(CDT) command is issued to build or refresh the dynamic class descriptor table, the class **profile-name** will not be added to the dynamic class descriptor table.

User response: Use the RALTER command to add a POSIT value to the profile before the SETROPTS RACLST(CDT) command is issued to build or refresh the dynamic class descriptor table.

**IRR52191I**  
Incorrect [ GROUP **group-name** ] **MEMBER** **member-name** ]. This name is already used by class **class-name**.

Explanation: You entered a class name on the GROUP or MEMBER suboperand of the CDTINFO keyword that is not valid. An incorrect GROUP name indicates that the class **class-name** specifies **group-name** on the GROUP or MEMBER suboperand. An incorrect MEMBER name indicates that the class **class-name** specifies **member-name** on the GROUP or MEMBER suboperand.

System action: If TSO prompting is active for the session, TSO prompts you to reenter the suboperand. If TSO prompting is not active, command processing stops.

User response: Reenter the suboperand correctly.

**IRR52192I**  
Incorrect [ MAXLENGTH | MAXLENX ] **value**. The valid range is 1 to 246.

Explanation: You entered a value for the specified suboperand that was not a number between 1 and 246, inclusive.

System action: If TSO prompting is active for the session, TSO prompts you to reenter the suboperand. If TSO prompting is not active, command processing stops.

User response: Reenter the suboperand correctly. It must be a number in the range 1 to 246.

**IRR52193I**  
Incorrect DEFaulTRc value. The valid values are 0, 4, and 8.

Explanation: You entered a value for the DEFaulTRc suboperand that was not 0, 4, or 8.

System action: If TSO prompting is active for the session, TSO prompts you to reenter the suboperand. If TSO prompting is not active, command processing stops.
User response: Reenter the suboperand correctly. It must be 0, 4, or 8.

**IRR52194I** Incorrect KEYQUALIFIERS value. The valid range is 0 to 123.

**Explanation:** You entered a value for the KEYQUALIFIERS suboperand that was not a number between 0 and 123, inclusive.

**System action:** If TSO prompting is active for the session, TSO prompts you to reenter the suboperand. If TSO prompting is not active, command processing stops.

User response: Reenter the suboperand correctly. It must be a number in the range 0 to 123.

**IRR52195I** Incorrect profile name profile-name. A class by this name is already defined in the class descriptor table supplied by IBM.

**Explanation:** A profile was defined in the CDT class which is a duplicate of a class name in the class descriptor table supplied by IBM (ICHRRCDX).

**System action:** Command processing continues, and the CDT profile is placed in the RACF database.

User response: Use the RDELETE command to delete the profile name before the SETROPTS RACLIST(CDT) command is issued to build or refresh the dynamic class descriptor table.

**IRR52196I** Incorrect profile name profile-name. USER, GROUP, and DATASET are reserved class names.

**Explanation:** A profile was defined in the CDT class with the name of a reserved class (USER, GROUP, or DATASET).

**System action:** Command processing continues, and the CDT profile is placed in the RACF database.

User response: Use the RDELETE command to delete the profile name before the SETROPTS RACLIST(CDT) command is issued to build or refresh the dynamic class descriptor table.

**IRR52197I** Warning: Class name class-name is a duplicate of a class in the installation-defined class descriptor table (ICHRRCDCE).

**Explanation:** A profile was defined in the CDT class which is a duplicate of a class name in the installation-defined class descriptor table (ICHRRCDCE). This is allowed so that the class entries in ICHRRCDE can be migrated to the dynamic class descriptor table.

**System action:** Command processing continues, and the CDT profile is placed in the RACF database.

User response: Use the RDELETE command to delete the profile name before the SETROPTS RACLIST(CDT) command is issued to build or refresh the dynamic class descriptor table.

**IRR52198I** Warning: The attribute class-attribute in class class-name may be in error. The value in the static definition (ICHRRCDCE) is value-1. The value in the dynamic definition is value-2.

**Explanation:** A CDTINFO segment was defined for a profile in the CDT class, and a class by that name is also in the installation-defined class descriptor table (ICHRRCDCE). This message is issued with IRR52197I if an attribute in the CDTINFO segment is different from the matching attribute in the existing class. If the dynamic class descriptor table is built or refreshed using the SETROPTS RACLIST(CDT) command, the dynamic definition of the class in the class descriptor table will override the static definition of the class in ICHRRCDE. Consequently, the class attribute will be changed from to value-1 to value-2.

**System action:** Command processing continues.

User response: Evaluate whether or not value-2 is the intended value of the class attribute. If it is not, use the RALTER command to change the class attribute value. When changing a class attribute, you must do careful planning to avoid unforeseen side effects. See z/OS Security Server RACF Security Administrator’s Guide for more information on changing attributes for an existing class.

**IRR52199I** Warning: Class name class-name does not contain a national character nor a number.

**Explanation:** A profile was defined in the CDT class with a name that does not conform to the recommended class name format. To assure IBM does not create an IBM-defined class in the future by this same name, you should choose a class name that contains at least one national character or a number.

**System action:** Command processing continues, and the CDT profile is placed in the RACF database.

User response: Use the RDELETE command to delete the profile name before the SETROPTS RACLIST(CDT) command is issued to build or refresh the dynamic class descriptor table.

**IRR52200I** [ GROUP | MEMBER ] name and profile name must be different. You must correct this error before the class profile-name can be added to the dynamic class descriptor table.

**Explanation:** A profile was defined in the CDT class, but the profile name is the same as the class specified.
for the GROUP or MEMBER suboperand.

**System action:** Command processing continues, and the CDT profile is placed in the RACF database. If the SETROPTS RACLST(CDT) command is issued to build or refresh the dynamic class descriptor table, the class profile-name will not be added to the dynamic class descriptor table.

**User response:** Use the RALTER command to change the GROUP or MEMBER name in the profile before the SETROPTS RACLST(CDT) command is issued to build or refresh the dynamic class descriptor table.

IRR52201I SIGNAL(YES) is not valid with RACLIST(DISALLOWED). You must correct this error before the class profile-name can be added to the dynamic class descriptor table.

**Explanation:** A profile was defined in the CDT class, but there are 2 mutually exclusive keywords defined in the profile. SIGNAL(YES) and RACLIST(DISALLOWED) cannot both be specified in the same profile.

**System action:** Command processing continues, and the CDT profile is placed in the RACF database. If the SETROPTS RACLST(CDT) command is issued to build or refresh the dynamic class descriptor table, the class profile-name will not be added to the dynamic class descriptor table.

**User response:** Use the RALTER command to change one of the named keywords in the profile before the SETROPTS RACLST(CDT) command is issued to build or refresh the dynamic class descriptor table.

IRR52202I MAXLENX value must be greater than or equal to the MAXLENGTH value. You must correct this error before the class profile-name can be added to the dynamic class descriptor table.

**Explanation:** A profile was defined in the CDT class, but the value for MAXLENX is less than the value for MAXLENGTH.

**System action:** Command processing continues, and the CDT profile is placed in the RACF database. If the SETROPTS RACLST(CDT) command is issued to build or refresh the dynamic class descriptor table, the class profile-name will not be added to the dynamic class descriptor table.

**User response:** Use the RALTER command to change one or both of the MAXLENX and MAXLENGTH values in the profile before the SETROPTS RACLST(CDT) command is issued to build or refresh the dynamic class descriptor table.

IRR52203I MEMBER and GROUP are mutually exclusive. You must correct this error before the class profile-name can be added to the dynamic class descriptor table.

**Explanation:** A profile was defined in the CDT class, but there are 2 mutually-exclusive keywords defined in the profile. Both MEMBER and GROUP cannot be specified in the same profile name.

**System action:** Command processing continues, and the CDT profile is placed in the RACF database. If the SETROPTS RACLST(CDT) command is issued to build or refresh the dynamic class descriptor table, the class profile-name will not be added to the dynamic class descriptor table.

**User response:** Use the RALTER command to change one of the named keywords in the profile before the SETROPTS RACLST(CDT) command is issued to build or refresh the dynamic class descriptor table.

IRR52204I Warning: segment-name segment is only valid for the class-name class.

**Explanation:** The named segment was specified on a profile for which the segment has no meaning. This message is issued for the CDTINFO segment and the ICTX segment. The CDTINFO segment is only meaningful for profiles in the CDT class. The ICTX segment is only meaningful for profiles in the LDAPBIND class.

**System action:** Command processing continues, and the profile is placed in the RACF database. The information in the segment will not be used in RACF processing.

**User response:** Delete the segment from the profile. For example, suppose you issued the following command:

```
RDEFINE DASDVOL VOL1 CDTINFO(POSIT(20))
```

You would then issue the following command to delete the segment:

```
RALTER DASDVOL VOL1 NODTINFO
```

IRR52205I Warning: CDTINFO is required for the CDT class.

**Explanation:** For RDEFINE, the profile was created, but the CDTINFO segment was not included in the definition. For RALTER, the segment was deleted. The CDTINFO segment is required for profiles in the CDT class, because information in the segment must be present before the profile can be used to define a class in the dynamic class descriptor table.

**System action:** Command processing continues, and the profile is added to or updated in the RACF database, but the profile may not have the wanted effect.
User response: Use the RALTER command to add the segment to the profile.

IRR52206I Unable to establish ESTAE environment.
Return code from ESTAE is return-code

Explanation: Dynamic parse was unable to establish an error recovery environment. Processing cannot continue without such an environment.

System action: Command processing stops. No action is taken.

User response: Notify your system programmer.

System programmer response: See “Problem Determination”.

Problem Determination: For a description of the ESTAE return code, see z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG.

IRR52207I The attribute class-attribute in class profile-name is in error. The value in the static definition (ICHRRCDE) is value-1. The value in the dynamic definition is value-2.

Explanation: A dynamic class, profile profile-name in the CDT class, was defined with the RDEFINE or RALTER command and the CDTINFO keyword. A class by that name is also in the installation-defined class descriptor table (ICHRRCDE). The attribute class-attribute in the definition of the dynamic class is not compatible with the matching attribute in the installation-defined class (also known as the static class definition). The attribute for the dynamic class must be changed to match value-1 in the static class definition; otherwise, the dynamic class will not be added to the dynamic class descriptor table.

System action: Command processing continues, and the CDT profile is placed in the RACF database. If the SETROPTS RACLIST(CDT) command is issued to build or refresh the dynamic class descriptor table, the class profile-name will not be added to the dynamic class descriptor table.

User response: Use the RALTER command to change the class attribute in the CDT profile named profile-name. For example, if the MEMBER attribute is in error, you would issue the following command to correct the error:

RALTER CDT profile-name CDTINFO(MEMBER(value-1))

For more information on moving an installation-defined class from ICHRRCDE to the dynamic class descriptor table, see z/OS Security Server RACF Security Administrator's Guide.

IRR52208I Incorrect | RSLKEY | TSLKEY | value. The valid range is 0 to maximum-value, or you may specify 99 to indicate all | resource | transaction | security level keys.

Explanation: You entered a value for the indicated keyword that was not 99 nor a number between 0 and the stated maximum number, inclusive.

System action: If TSO prompting is active for the session, TSO prompts you to reenter the suboperand. If TSO prompting is not active, command processing stops.

User response: Reenter the suboperand correctly. It must be either 99 or a number in the indicated range.

IRR52209I Incorrect | RSLKEY | TSLKEY | value. You cannot specify key-value in a list of keys.

Explanation: You entered a value for the indicated keyword that cannot be specified along with other keys.

System action: Command processing stops, and all of the values specified are ignored.

User response: Reenter the suboperand correctly. It must be specified alone, without other key values.

IRR52210I Incorrect MAPPINGTIMEOUT value. The valid range is 1 to 3600.

Explanation: You entered a value for the MAPPINGTIMEOUT keyword that was not a number between 1 and 3600, inclusive.

System action: If TSO prompting is active for the session, TSO prompts you to reenter the suboperand. If TSO prompting is not active, command processing stops.

User response: Reenter the suboperand correctly. It must be a number in the range 1 to 3600.

IRR52211I The IRRDPI00 LIST command encountered an error. parameter is not valid.

Explanation: The value specified for parameter is not valid. The combination of profile type, segment name (if specified), and keyword name (if specified) was not found in the dynamic parse table. For more information about valid values for profile type, segment name, and keyword name, see the description of the IRRDPI00 command in z/OS Security Server RACF System Programmer's Guide.

System action: Command processing terminates.

User response: Reissue the command and specify a valid value for the LIST operand.
Warning: GENERIC(ALLOWED) is ignored for profile profile-name because MEMBER was also specified.

Explanation: A profile was defined in the CDT class to represent a grouping class (MEMBER was specified), and GENERIC(ALLOWED) was specified or defaulted. Because generic processing is not allowed for a grouping class, GENERIC(ALLOWED) will be ignored if class profile-name is added to the dynamic class descriptor table.

System action: Command processing continues, and the CDT profile is placed in the RACF database. If the SETROPTS RACLIST(CDT) command is issued to build or refresh the dynamic class descriptor table and the class profile-name is added to the dynamic class descriptor table, the GENERIC(ALLOWED) keyword will be ignored, because generic processing is not allowed for a grouping class.

User response: Use the RALTER command to specify GENERIC(DISALLOWED) for CDT profile profile-name to reflect the proper setting for a grouping class.

keyword-1 is not valid with keyword-2. You must correct this error before the class profile-name can be added to the dynamic class descriptor table.

Explanation: A profile was defined in the CDT class, but there are two mutually exclusive keywords defined in the profile. The two named options cannot both be specified in the same profile. For example, GENERIC(DISALLOWED) cannot be specified with GENLIST(ALLOWED).

System action: Command processing continues, and the CDT profile is placed in the RACF database. If the SETROPTS RACLIST(CDT) command is issued to build or refresh the dynamic class descriptor table and the class profile-name will not be added to the dynamic class descriptor table.

User response: Use the RALTER command to change one of the named keywords in the profile before the SETROPTS RACLIST(CDT) command is issued to build or refresh the dynamic class descriptor table.

Warning: USEMAP=NO, DOMAP=NO, and MAPREQUIRED=YES is not a valid configuration.

Explanation: The combination of values for USEMAP, DOMAP, and MAPREQUIRED is not valid and will result in an error from the identity cache. When MAPREQUIRED is set to YES, either USEMAP or DOMAP must also be set to YES.

System action: Command processing continues and the profile is added to or updated in the RACF database, but it specifies a configuration that is not supported by the identity cache. This configuration will cause the identity cache to reject all attempts to store identity context information.

User response: Use the RALTER command to specify a valid combination of values for USEMAP, DOMAP, and MAPREQUIRED. See z/OS Integrated Security Services EIM Guide and Reference for more information about configuring the identity cache.

The attribute keyword-1 in class class-1 is not compatible with the attribute keyword-2 in class class-2 because the classes share a POSIT number.

Explanation: The profile class-1 was defined or updated in the CDT class, and an error was found in the definition of the dynamic class because the class shares a POSIT number with another class. The specified keyword-1 is not compatible with the corresponding keyword in the class with the shared POSIT number (class-2). For example, this message will be issued if a profile is defined or updated in the CDT class with GENERIC(DISALLOWED) specified, and the class shares a POSIT number with an existing class that specifies GENERIC(ALLOWED).

System action: Command processing continues and the CDT profile is placed in the RACF database. If the SETROPTS RACLIST(CDT) command is issued to build or refresh the dynamic class descriptor table and class class-1 is added to the dynamic class descriptor table, the value of the specified keyword may be changed to match the class with the shared POSIT number. For example, if GENERIC(DISALLOWED) is specified for class-1, and class-2 specifies GENERIC(ALLOWED), then class-1 may be changed to GENERIC(ALLOWED), and generic processing will be allowed for class-1. For more information, see the description of keyword-1 on the RALTER command in the z/OS Security Server RACF Command Language Reference.

User response: Use the RALTER command to change either CDT profile class-1 or class-2 so they specify keywords that are compatible. Alternatively, if class-1 is a new dynamic class, you can use the RALTER command to change the POSIT number in CDT profile class-1 to a POSIT number that is not shared with class-2. For more information about creating a dynamic class that shares a POSIT number, see the z/OS Security Server RACF Security Administrator’s Guide.

An error was detected in the definition of custom field profile-name.

error-description

Explanation: This error message is issued by the RDEFINE, RALTER, or IRRDPI00 command. An error was found in the definition of the specified custom field profile in the CFIELD class. The keywords for the CFDEF segment define the attributes of a custom field, and there were conflicts detected between several keywords. The possible values of error-description are:
• MAXVALUE is less than MINVALUE.
• MAXVALUE has more digits than allowed by MAXLENGTH.
• MINVALUE has more digits than allowed by MAXLENGTH.
• FIRST(xxx) does not match TYPE(xxx).
• OTHER(xxx) does not match TYPE(xxx).
• MAXLENGTH is missing or incorrect for a field with TYPE(xxx).
• MAXVALUE must be specified for a field with TYPE(NUM).
• NOMAXVALUE must be specified for a field with TYPE(xxx).
• MINVALUE must be specified for a field with TYPE(NUM).
• NOMINVALUE must be specified for a field with TYPE(xxx).
• MIXED(NO) must be specified for a field with TYPE(xxx).
• TYPE(xxx) is not a valid type.

For more information on custom fields, see the z/OS Security Server RACF Security Administrator’s Guide. For more information on each keyword in the CFDEF segment, see the RDEFINE and RALTER commands in the z/OS Security Server RACF Command Language Reference.

System action: Command processing continues. The specified custom field cannot be used as a valid keyword on RACF commands until the error is corrected and the IRRDPI00 UPDATE command is issued or reissued.

User response: The value of error-description describes the error that must be corrected. If you issued the RDEFINE or RALTER command, you must issue the RALTER command to correct the error. If you issued the IRRDPI00 command, you must correct the CFIELD profile definition with the RALTER command, or by deleting it and redefining it, before reissuing the IRRDPI00 command.

For example, if you issued an RDEFINE command and you see the following messages:
• IRR52216I An error was detected in the definition of custom field USER.CSDATA.EMPSER. FIRST(ALPHA) does not match TYPE(NUM).
• IRR52216I An error was detected in the definition of custom field USER.CSDATA.EMPSER. OTHER(ALPHA) does not match TYPE(NUM).

You must issue the following command to correct the errors:

RALTER CFIELD USER.CSDATA.EMPSER CFDEF(FIRST(NUMERIC) OTHER(NUMERIC)).
### RACF cross-reference utility (IRRUT100) messages

<table>
<thead>
<tr>
<th>Code</th>
<th>Message Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRR61000I</td>
<td>Open failed for dd ddn</td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>The RACF cross-reference utility program was unable to open the data set specified by the specified ddname.</td>
</tr>
<tr>
<td><strong>System programmer response:</strong></td>
<td>To recover from the problem, ensure that the DD statement is correct.</td>
</tr>
<tr>
<td><strong>Problem Determination:</strong></td>
<td>Check for other errors related to the disk pack on which the data set resides.</td>
</tr>
<tr>
<td>IRR61001I</td>
<td>Invalid input (80 character input record)</td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>A name supplied as input to the cross-reference utility program has more than 8 characters. The remaining records are scanned for errors.</td>
</tr>
<tr>
<td><strong>System action:</strong></td>
<td>The utility program stops.</td>
</tr>
<tr>
<td>IRR61002I</td>
<td>Unauthorized user</td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>You are not defined to RACF or do not have sufficient authority to run the cross-reference utility program.</td>
</tr>
<tr>
<td><strong>User response:</strong></td>
<td>See your RACF security administrator.</td>
</tr>
<tr>
<td>IRR61003I</td>
<td>Following names were not processed</td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>More than 1000 names were specified to the cross-reference utility program.</td>
</tr>
<tr>
<td><strong>System action:</strong></td>
<td>Those names over 1000 are listed and are not processed.</td>
</tr>
</tbody>
</table>

### RACF database verification (IRRUT200) messages

<table>
<thead>
<tr>
<th>Code</th>
<th>Message Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRR62001I</td>
<td>Unable to open DD ddn - processing terminated</td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>The verification utility program was not able to open the database with the specified ddname.</td>
</tr>
<tr>
<td><strong>System action:</strong></td>
<td>Processing stops.</td>
</tr>
<tr>
<td><strong>System programmer response:</strong></td>
<td>To recover from the problem, ensure that the DD statement is correct.</td>
</tr>
<tr>
<td><strong>Problem Determination:</strong></td>
<td>Check for other errors related to the disk pack on which the database resides.</td>
</tr>
<tr>
<td>IRR62002I</td>
<td>Unable to open DD SYSUT1 - copy function bypassed</td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>The verification utility program was not able to open the SYSUT1 data set.</td>
</tr>
<tr>
<td><strong>System action:</strong></td>
<td>The data set associated with DD SYSRACF has opened successfully and is used by the utility program.</td>
</tr>
<tr>
<td>IRR62003I</td>
<td>Unable to open dd SYSRACF - SYSUT1 must contain RACF data set</td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>The verification utility program cannot open the SYSRACF data set. The data set associated with DD SYSUT1 is assumed to contain a copy of the RACF database.</td>
</tr>
<tr>
<td><strong>System action:</strong></td>
<td>Processing continues.</td>
</tr>
<tr>
<td><strong>Programmer response:</strong></td>
<td>The database verification utility continues to process if it was unable to open the data set pointed to by SYSRACF DD statement. The utility assumes that the work data set (SYSUT1) contains a copy of the RACF database. Make sure that</td>
</tr>
</tbody>
</table>
SYSRACF DD statement points to a RACF data set.

**IRR62004I** Insufficient storage - processing terminated

**Explanation:** A GETMAIN failed for the buffers and work areas necessary for the verification utility program to function. The request was for storage from subpool 0.

**System action:** Processing stops.

**Programmer response:** Get the message ID, any diagnostic information generated and contact your IBM support center.

**Problem Determination:** A GETMAIN was issued for internal work areas (buffers and work tables) in the IRRUT200 utility. The GETMAIN was unsuccessful. Probable cause: the storage was unavailable.

**IRR62007I** Invalid control statement

**Explanation:** The verification utility program found that the control statement contains a delimiter or contents errors.

**System action:** Processing stops.

**Programmer response:** Verify that the SYSIN DD statement contains valid IRRUT200 control statements. For valid control statements, see [z/OS Security Server RACF System Programmer's Guide](#).

**IRR62008I** I/O ERROR - jji, sss, ddd, devtyp, ddn, oper, err, xxxx, acc

**Explanation:** The verification utility program encountered a permanent I/O error while processing on device ddd. In the message text, the error analysis information provided by the SYNADAF data management macro instruction issued by the SYNAD routine was:

- jji: Job name
- sss: Step name
- ddd: Unit address of the device
- devtyp: Device type
- ddn: Data definition name
- oper: Operation attempted
- err: Error description
- xxxx: Last seek address or block count
- acc: Access method

This message can be caused by unformatted space at the end of the RACF database. Copying the RACF database with utilities other than IRRUT400 can cause unformatted space.

**System action:** Utility processing stops.

**User response:** Copy the database with IRRUT400 to format the space.

**IRR62009I** EOF on SYSIN - processing terminated

**Explanation:** The verification utility program found an unexpected end-of-file condition on the SYSIN data set.

**System action:** Processing stops.

**Programmer response:** Ensure that the END control statement is included in the SYSIN DD control statements to prevent an implied end of utility processing from occurring.

**IRR62010I** RACF data set not found - processing terminated

**Explanation:** A failure occurred when the verification utility program made a request to dynamic allocation for information retrieval.

**System action:** Processing stops.

**Programmer response:** Make sure that SYSRACF DD statement specifies, as the data set name, the database you want to use during processing.

**IRR62012I** Insufficient storage for map function - request terminated

**Explanation:** A GETMAIN failed for the storage required by the verification utility program to perform the map function. The request was for storage from subpool 0.

**System action:** Processing stops.

**Programmer response:** This is an internal error. Get the message ID, any diagnostic information generated, and contact your IBM support center.

**Problem Determination:** A GETMAIN request was done for storage to process the BAM/allocation verification for the MAP function of the IRRUT200 utility. The GETMAIN failed. The probable cause is unavailable storage.

**IRR62014I** RBA of top level index block is invalid - may be an empty dataset - processing terminated

**Explanation:** The verification utility program found an error in the RBA (relative byte address) of the top-level index block (in the ICB).

**System action:** Processing stops.

**Programmer response:** See “Problem Determination” for more detail. Use the BLKUPD command to correct the RBA of the top-level index block. Also, make sure that the database is not empty.

**Problem Determination:** When this error occurs, the utility dumps the ICB in hexadecimal. Any one of the following conditions can cause this error in the ICB:

- The first 2 bytes are not zero.
- The last 4 bytes are zero.
The last 12 bits are not zero (denoting an address not on a 4K boundary).

IRR62015I RBA of first BAM block is invalid - map function terminated

Explanation: The verification utility program found an error in the RBA (relative byte address) of the first BAM block (in the ICB).

System action: Processing stops.

Programmer response: See “Problem Determination” for more detail. Use the BLKUPD command to correct the RBA of first BAM block.

Problem Determination: When this error occurs, the utility dumps the ICB in hexadecimal. Any one of the following conditions can cause this error in the BAM:

- The last 4 bytes are zero.
- The first 2 bytes are not zero.
- The last 12 bits are not zero (denoting an address not on a 4K boundary).

IRR62017I Sequence set chain field is broken

Explanation: In processing all the index blocks, the verification utility program keeps a count of level 01 blocks. This count is used while processing the sequence set. While following the chain of level 01 blocks (sequence set), the utility program found a zero sequence set RBA (relative byte address) before the count of level 01 blocks was reached.

System action: Utility processing stops.

Programmer response: The current index block is dumped in hexadecimal. Use the BLKUPD command to correct the problem. Rerun the IRRUT200 utility.

IRR62018I Program limit exceeded - processing of index blocks terminated

Explanation: More than six levels of index blocks were found by the verification utility program.

System action: Index block processing stops. After six levels have been processed, Level 01 blocks are not processed.

Programmer response: Use the BLKUPD command to confirm that you have as many levels as reported by this message. If you do confirm this error, split the RACF database (using the range table) to correct the problem. For more information, see z/OS Security Server RACF Diagnosis Guide. If you cannot correct the problem, contact your IBM support center.

IRR62019I Unable to open DD SYSUT1 for READ after COPY function completed - processing terminated

Explanation: The RACF database verification utility program was not able to open the SYSUT1 data set for read after successfully copying the RACF database. The RACF database is defined by the SYSRACF DD statement.

System action: Utility processing stops.

Programmer response: Check for disk pack error messages related to SYSUT1 DD allocation; verify the characteristics of the data set for SYSUT1 and make sure that they are correct. Rerun the IRRUT200 utility using the SYSUT1 data set for SYSRACF DD statement and a work data set for SYSUT1. If the problem still occurs, run the IRRUT200 utility with the original database used before the error and do not use the copy function.

IRR62021I Unable to load class descriptor table

Explanation: The verification utility program was not able to load the class descriptor table.

System action: The verification utility program continues processing general classes by using their class ID numbers instead of their class names.

IRR62023I Incorrect RACF dataset format

Explanation: One of the following problems occurred:

- The database name pointed to by the new format RACF database field (ICBDSCOMT) of the inventory control block (ICB) for the SYSRACF DD statement is not a valid database.
- The inventory control block (ICB) does not have the correct information in the ICBID field.

System action: Processing stops.

Programmer response: Verify that your SYSRACF DD statement points to a database that was pre-formatted by RACF database initialization utility (IRRMIN00). Correct the problem and rerun the IRRUT200 utility.

Problem Determination: Make sure that the database was initialized by the IRRMIN00 utility.
**IRR62024I** Segment table cannot be read

**System action:** Processing stops.

**Programmer response:** Verify that your SYSRACF DD statement points to a database that was pre-formatted by RACF database initialization utility (IRRMIN00). Correct the problem and rerun the IRRUT200 utility.

**Problem Determination:** An attempt was made by the RACF Database Verification utility to read the segment table associated with the templates for the data set specified by SYSRACF DD statement. The READ was unsuccessful because of one of the following reasons:

- The database was not properly initialized by RACF Database Initialization utility (IRRMIN00).
- Reading of the database resulted in an end-of-file condition before the segment table was found.
- The segment table did not exist.

Ensure that the database is initialized and contains a set of templates and the associated segment table.

**IRR62025I** Name of segment or profile in index does not match equivalent in profile.  See the following.

**Explanation:** The name or type of the profile do not agree between the index entry and the contents of the profile read. The profile segment type might be unknown. This message includes the following information about the error:

- **Prof Type:** profile type
- **Seg Name in Prof:** segment name in the profile
- **Seg Name in Index:** segment name in the index
- **Prof Name in Prof:** profile name in the profile
- **Prof Name in Index:** profile name in the index

For example, in the following example, the profile names do not match:

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRR62025I Prof Type: DATA SET</td>
<td>Segment type does not match.</td>
</tr>
<tr>
<td>IRR62025I Seg Name in Prof: BASE</td>
<td>Profile segment name does not match.</td>
</tr>
<tr>
<td>IRR62025I Seg Name in Index: BASE</td>
<td>Index segment name does not match.</td>
</tr>
<tr>
<td>IRR62025I Prof Name in Prof: PAYROLL.JULY.1987</td>
<td>Profile name does not match.</td>
</tr>
<tr>
<td>IRR62025I Prof Name in Index: PAYROLL.JULY.1986</td>
<td>Index name does not match.</td>
</tr>
</tbody>
</table>

**System action:** Processing continues.

**Programmer response:** Use the BLKUPD command to correct the inconsistency. Check to make sure that the templates on the database are not downlevel. At IPL, check for message ICH579E in the system log. Run IRRMIN00 PARM=UPDATE to correct the problem.

**Problem Determination:** The error message indicates the index name and profile name in which the mismatch was found. Use this information to correct the inconsistency.
IRR62030I  Data block failed validity check
Explanation: The data block pointed to by a level one index block does not begin with the value X'83'.
System action: Processing stops.
Programmer response: This is an internal error. The block in error is dumped in hexadecimal. Collect the message ID, dump, and any other diagnostic materials and contact your IBM support center.

IRR62031I  Data block key length invalid
Explanation: The record name in the profile is not from 1 to 255 bytes in length.
System action: Processing stops.
Programmer response: This is an internal error. The block in error is dumped in hexadecimal. Collect the message ID, dump, and any other diagnostic material and contact your IBM support center.

IRR62032I  Displacement to free space is incorrect
Explanation: The offset (in the header of the index block) to the free space in the block is incorrect, or the end-of-block delimiter (X'0C') is not present.
System action: Utility processing stops.
Programmer response: This is an internal error. The particular index block is dumped in hexadecimal. Collect the message ID, dump, and any other diagnostic material and contact your IBM support center.

IRR62033I  Displacement to last key is incorrect
Explanation: The offset (in the header of the index block) to the last entry is incorrect, or the entry identifier (X'21' or X'20') is not present.
System action: Utility processing stops.
Programmer response: This is an internal error. The index block is dumped in hexadecimal. Collect the message ID, dump, and any other diagnostic material and contact your IBM support center.

IRR62034I  E(P) Byte/RBA of next block in sequence set is invalid
Explanation: The sequence set pointer entry in the level one index block is not preceded by the value X'6x', or the next level one block is not valid for one of the following reasons:
- The first 2 bytes are not zero.
- The last 4 bytes are zero.
- The RBA is not a multiple of 4096.
System action: Utility processing stops.
Programmer response: The index block is dumped in hexadecimal. Use the BLKUPD command to correct the problem in the index. Rerun the IRRUT200 utility.

IRR62035I  E(P) Byte/RBA xxxxxxxxxx Failed validity check
Explanation: The pointer entry of an index entry in the block is not preceded by the value X'6x', or the RBA xxxxxxxxxx of the next level index block or profile is not valid for one of the following reasons:
- The first 2 bytes are not zero.
- The last 4 bytes are zero.
- The RBA is not a multiple of 4096.
- For level one blocks, the RBA is not a multiple of 256.
System action: Utility processing stops.
Programmer response: If the RBA was not valid, no dump is produced. Otherwise, a hexadecimal dump is produced. Use the BLKUPD command to correct the problem.

IRR62036I  End of data flag byte possibly missing
Explanation: The end-of-block delimiter at the end of the index block is not X'0C' or the displacement to this byte is incorrect. The displacement is calculated by adding the sum of the length of the last entry name in the block and the length of the pointer entry to the offset of the last entry name in the block. If the length of the entry name is incorrect, the displacement to this byte is incorrect.
System action: Utility processing stops.
Programmer response: The block in error is dumped in hexadecimal. Use the BLKUPD command to correct the problem. Rerun the IRRUT200 utility.

IRR62037I  Following Level 01 block is not pointed to by a Level 02 block
Explanation: An index block with a level greater than X'02' points to an index block with a level of X'01' in the header. IRRUT200 processes the level one index block normally.
System action: Processing continues.
Programmer response: The level one index block was processed. You might want to run the IRRUT200 utility against your database again to check for any remaining errors.
IRR62038I  I/O error rereading BAM block - map function terminated

Explanation:  IRRUT200 encountered an unrecoverable I/O error while attempting to reread a BAM block. The block is not dumped.
System action:  MAP function stops.
Programmer response:  An I/O error message was generated before this message (IRR62008I). Use this message to determine the cause of the I/O error.

IRR62039I  Index block failed validity check

Explanation:  The block does not begin with the value X'8A'.
System action:  Utility processing stops.
Programmer response:  Use the BLKUPD command to confirm this error. If you confirm this error, correct the problem using BLKUPD. For more information, see [z/OS Security Server RACF Diagnosis Guide](#). If you cannot correct the problem, contact your IBM support center.

IRR62040I  Invalid E(K) byte in key entry at offset

Explanation:  An index entry name might not be preceded by a valid key byte. All entries in index blocks that are not level one must begin with the value X'21'. In level one index blocks, either X'22' or X'21' must precede each entry except for the last entry, which must be preceded by X'20'.
System action:  Processing continues.
Programmer response:  Use the BLKUPD command to correct the problem.

IRR62041I  Key entry length invalid at offset offset

Explanation:  An index entry name does not have a valid length. An entry other than the first entry in a block that is not level one, might have a zero length. If it does, it must also have a compression count other than zero. The compression count must not be greater than the length of the first entry in the block. The offset indicated in the message is the offset of the beginning of the incorrect entry in the index block.
System action:  Utility processing stops.
Programmer response:  Use the BLKUPD command to confirm this error. If you do confirm this error, correct the problem by using BLKUPD. For more information, see [z/OS Security Server RACF Diagnosis Guide](#). If you cannot correct the problem, contact your IBM support center.

IRR62042I  Logical length of data block is invalid

Explanation:  The logical length of the profile is not a multiple of 256 or is greater than the allocated length as defined in the header.
System action:  Utility processing stops.
Programmer response:  Use the BLKUPD command to confirm this error. If you do confirm this error, correct the problem by using BLKUPD. For more information, see [z/OS Security Server RACF Diagnosis Guide](#). If you cannot correct the problem, contact your IBM support center.

IRR62043I  More than 200 BAM allocation errors found

Explanation:  In verifying the BAM blocks with the actual allocation of segments in the RACF database, IRRUT200 found more than 200 locations with possible conflicts.
System action:  Utility processing stops.
Programmer response:  Make sure that you are processing with the correct database. Also, ensure that you have a database at the right release level and properly initialized.

IRR62044I  Non Level 01 index block is in sequence set

Explanation:  The index block is in the sequence set, but the level in the header is not one.
System action:  Processing stops.
Programmer response:  The block in error is dumped in hexadecimal. Use the BLKUPD command to correct the problem.

IRR62045I  Possible compression count error in key entry at offset offset

Explanation:  An index entry name might not have a valid compression count. The first entry must have a zero compression count. An entry, other than the first entry, must have a compression count that is less than or equal to the length of the first entry name. The offset indicated in the message is the offset of the beginning of the incorrect entry in the index block.
System action:  Processing continues.
Programmer response:  At the completion of the utility processing, you can use the offset from the message and correct the problem by using BLKUPD command.
IRR62046I Possible loop in sequence set
Explaination: The first entry name of the level one
index block is not alphabetically greater than the first
entry name of the previous level one index block.
System action: Utility processing stops.
Programmer response: Use the BLKUPD command to
confirm this error. If you do confirm this error, correct
the problem by using BLKUPD. Note that if both
blocks contain X'22', they are valid duplicates. For more
information, see z/OS Security Server RACF Diagnosis
Guide. If you cannot correct the problem, contact your
IBM-support center.

IRR62048I RBA invalid for template at offset offset
RBA rba
Explanat: In the ICB, the indicated RBA for the
template at the indicated offset is not valid. The RBA is
not valid for one of the following reasons:
• The first 2 bytes are not zero.
• The last 4 bytes are zero.
• The RBA is not a multiple of 4096.
System action: Processing continues.
Programmer response: A dump is provided in
hexadecimal. Use the BLKUPD command to correct the
problem.

IRR62050I RBA of first block of index sequence set
is invalid
Explanat: The RBA of the first block of the index
sequence set (in the ICB) is not valid for one of the
following reasons:
• The first 2 bytes are not zero.
• The last 4 bytes are zero.
• The RBA is not a multiple of 4096.
System action: Processing stops.
Programmer response: A dump is provided for the
block in error. Use the BLKUPD command to correct the
problem.

IRR62051I RBA of next BAM block is invalid -
map function terminated
Explanat: The RBA of the next BAM block is not
valid for one of the following reasons:
• The first 2 bytes are not zero.
• The RBA is not a multiple of 4096.
System action: Map function stops. A hexadecimal
dump is provided.
Programmer response: Using the information from the
explanation and the dump, use the BLKUPD command to
correct the problem.

IRR62053I Read failed for top level index block -
processing terminated
Explanat: A permanent I/O error occurred while
attempting to read the top-level index block. The block
is not dumped.
System action: Processing stops.
Programmer response: Message IRR62008I contains
the specifics regarding the I/O error. Use this
information to determine the cause of the problem.

IRR62055I Template count in ICB is invalid
Explanat: The ICB contains a count of the number of
templates that is either zero or greater than the
number of spaces allocated for template definitions.
System action: Processing stops.
Programmer response: Make sure that your database
has been properly initialized by RACF Database
Initialization Utility (IRRMIN00). Also, make sure the
SYSRACF DD statement points to the correct database.

IRR62056I Top level index block failed validity
check - processing terminated
Explanat: The top-level index block, pointed to by
the ICB, does not begin with the value X'8A'.
System action: Processing stops.
Programmer response: Make sure that your database
has been properly initialized by the RACF Database
Initialization Utility (IRRMIN00). Also, make sure that
SYSRACF DD statement points to the correct database.

IRR62057I Unrecoverable logic error detected
during name verification
Explanat: An error occurred within the utility.
System action: Processing stops.
Programmer response: Report this problem to your
IBM support center.

IRR62058I The offset table pointer for the above
index block failed a validity check
Explanat: This message is issued as part of the
validity checking done by this utility.
Programmer response: Use the BLKUPD command to
investigate and correct the error.

IRR62059I The offset table entry count for the
above index block failed a validity check
Explanat: This message is issued as part of the
validity checking done by this utility.
Programmer response: Use the BLKUPD command to investigate and correct the error.

IRR62060I The count of names in the above index block statistics does not equal the offset table count of count.

Explanation: This message is issued as part of the validity checking done by this utility.

Programmer response: Use the BLKUPD utility to investigate and correct the error.

IRR62061I The offset table pointer at index position position has failed a validity check for the above index block.

Explanation: This message is issued as part of the validity checking done by this utility.

Programmer response: Use the BLKUPD command to investigate and correct the error.

IRR62062I The offset table pointer at index position position does not point to a valid entry in the above index block.

Programmer response: Use the BLKUPD command to investigate and correct the error.

IRR62063I Zero segment count found during [MAP | INDEX] processing for entry at offset offset.

Explanation: A segment count of zero was detected in an index entry beginning at offset offset. This is an incorrect state in that all index entries should have one or more segments.

System action: Utility processing continues. A return code of 8 is issued. BAM allocation errors (BAM=ALLOC ACTUAL=UNALLOC) are flagged during MAP processing for valid entries in the block containing the failing entry.

For index processing, statistics are not compiled for the failing index block. Validation continues with the next index entry.

Map processing stops for the failing block. It continues with the next block.

Programmer response: A dump is provided for the index block in error if INDEX was requested. The offset of the index entry containing the incorrect segment count is included in this message text. (If only MAP processing was requested, running IRRUT200 another time requesting INDEX FORMAT can help identify the block in which the error occurred.) Determine whether it is easier to delete or correct this entry. In either case, see z/OS Security Server RACF Diagnosis Guide for index entry formats.

If it is decided that the entry should be deleted, do so by using the BLKUPD command. After deletion, MAP processing shows BAM allocation errors (BAM=ALLOC ACTUAL=UNALLOC) for the BAM associated with the deleted profile. These errors can be resolved by using the RACF database utility (IRRUT400).

If it is decided that the entry should be corrected, do so by using BLKUPD.

Upon completion of index entry correction or deletion, IRRUT200 must be run against the updated database to ensure complete validation. IRRUT200 bypasses validation for index entries containing a zero segment count. Data block verification is bypassed during map processing for all entries in the data block following the entry in error.

IRR62064I Serialization is not held while verifying the database associated with DD SYSUT1.

Explanation: This is an informational message. It appears at the end of the DD SYSUT2 data set only when the SYSUT1 DD statement is specified and the SYSRACF DD statement is absent from your JCL.

Programmer response:

- If the IRRUT200 utility ran without errors, the message is informational only; no response is needed.
- If the DD SYSUT1 data set has specified the active database, and database updates were performed while the IRRUT200 utility was running, database errors might have been reported. Database errors reported in this instance are not necessarily true database errors. Either rerun the job without making database updates while the job is running, or specify a DD SYSRACF statement to take advantage of the serialization on the data set.

IRR62065I IEBGENER copied SYSRACF to the work data set SYSUT1, IEBGENER RC=return_code.

Explanation: When a SYSUT1 DD statement is specified, IRRUT200 links to the MVS utility IEBGENER. IEBGENER copies the database pointed to by the SYSRACF DD statement to a work data set pointed to by the SYSUT1 DD statement. A return code of 0 or 4 indicates that IEBGENER successfully copied the database. However, a return code of 4 indicates some mismatch in the output and input data set attributes.

System action: With the work data set copied, the verification of the database continues.

User response: For a return code of 4, correct the data set pointed to by the SYSUT1 DD statement so that it has the same attributes as the database pointed to by the SYSRACF DD statement.
IRR62066I  IEBGENER failed to copy SYSRACF to the work data set SYSUT1, IEBGENER RC=return_code

Explanation: When a SYSUT1 DD statement is specified, IRRUT200 links to the MVS utility IEBGENER. IEBGENER copies the database pointed to by the SYSRACF DD statement to a work data set pointed to by the SYSUT1 DD statement. IEBGENER cannot copy the database and IRRUT200 ends processing.

System action: IRRUT200 ends processing.

User response: See the appropriate MVS documentation for an explanation of the IEBGENER return codes. Correct the problem and resubmit the job.

IRR62067I  Database copy (SYSRACF to SYSUT1) failed due to incompatible device types.

Explanation: The database (SYSRACF) and work data set (SYSUT1) have incompatible device types.

System action: Processing ends with a return code of 12.

Programmer response: Do one of the following tasks:

- Use the RACF Database Split/Merge/Extend utility program (IRRUT400) to copy a database to or from devices with different track geometries.
- Create a work data set (SYSUT1) on a device that is compatible with the database you are copying (SYSRACF).

Run the IRRUT200 utility again.

IRR62068I  Base profile structure of alias entry contains an error.

Explanation: An error was found in the base profile structure of an alias index entry. The structure should contain the number of base profiles that correspond to this alias name, followed by the length and name of each base profile. The count of base profiles might not match the actual number of entries in the structure, or the length of an entry might be incorrect.

System action: The block containing the error is printed, and utility processing continues with the next block.

Programmer response: Use the BLKUPD command to confirm and correct the problem. For more information, see the z/OS Security Server RACF Diagnosis Guide.

IRR62069I  Database copy and activation failed.

Explanation: SYSRACF does not identify the active primary RACF data set, or the SYSRACF or SYSUT1 statement was not specified.

System action: Processing ends with a return code of 12 (X'C').

Programmer response: Issue RVARY LIST on the system to determine the name and state of the primary and backup RACF data sets and their volume serial numbers. If the backup is not currently inactive, issue RVARY INACTIVE to deactivate it. Ensure that SYSUT1 and SYSRACF specify the correct data set names and volume serial numbers, or that they point to data sets that are correctly cataloged if the volume is not specified. Correct the SYSRACF and SYSUT1 DD statements as needed, and run the IRRUT200 utility again. If you only intended to make a copy of the RACF database, and not activate the backup data set, omit PARM=ACTIVATE from the EXEC statement.

IRR62070I  Backup data set activated on this system only. Synchronization of primary and backup cannot be guaranteed.

Explanation: This is an informational message. It appears when PARM=ACTIVATE is specified and the target of the copy is on a shared device but the system is not in RACF sysplex communications mode. The backup data set has been activated on this system, but it might not have been activated on all systems necessary to maintain synchronization of the primary and backup data sets.

System action: Utility processing continues.

Programmer response:

- If the backup data sets is not shared by other systems, the message is informational only; no response is needed.
- If the SYSUT1 data set is an inactive backup on other sharing systems, activate it immediately by issuing RVARY ACTIVE on the sharing systems.

IRR62071I  SYSIN DD statement ignored. PARM=ACTIVATE has been specified.

Explanation: This is an informational message. When PARM=ACTIVATE is specified on the EXEC statement, the control statements specified as SYSIN, if any, are not processed and only the copy function is executed.

System action: Utility processing continues.

Programmer response: None. Verification of the input data set specified by SYSRACF should be done before copying it into the inactive backup.
IRR62072I  Database copy (SYSRACF to SYSUT1) failed. SYSUT1 is an active RACF data set.

Explanation: A copy of the RACF data set has been requested and the output data set is an active primary or backup data set on this system.

System action: Processing ends with a return code of 12 (X'C').

Programmer response: Do one of the following tasks:

- If you are making a copy of the RACF database for archiving or for analysis, correct your SYSUT1 DD statement to point to a work data set and run the IRRUT200 utility again.
- If you are attempting to synchronize the primary and backup data sets, see Chapter 1 "Copying your database" in the z/OS Security Server RACF System Programmer's Guide.

IRR62073I  Database copy (SYSRACF to SYSUT1) failed. Same data set specified for input and output.

Explanation: A copy of the RACF data set has been requested but the SYSRACF and SYSUT1 DD statements point to the same data set. IRRUT200 does not copy a data set over itself.

System action: Processing ends with a return code of 12 (X'C').

Programmer response: Correct your DD statements to point to the correct data sets and run the IRRUT200 utility again.

IRR62074I  RVARY ACTIVE failure against SYSUT1, RC = return-code

Explanation: The ACTIVATE parameter was specified, requesting that the backup data set be activated after the copy has completed. An RVARY ACTIVE was attempted, but ended with the decimal return code indicated in the message.

System action: Utility processing ends with a return code of 8.

Programmer response: Check the job output for additional RVARY error messages.

IRR62075I  service on dname failure, RC = return-code

Explanation: RACF invoked the dynamic allocation (DYNALLOC) or the catalog locate (LOCATE) service for the DDNAME SYSRACF or SYSUT1. The service returned an unexpected return code as indicated by the decimal return code in the message.

System action: Utility processing ends with return code 12 (X'C').

Programmer response: Check the information specified on the DD statement if the name in the message is SYSRACF or SYSUT1. Check that the indicated data set is cataloged correctly. For additional information about DYNALLOC return codes, see z/OS MVS Programming: Authorized Assembler Services Guide Interpreting DYNALLOC Return Codes. For additional information about LOCATE return codes, see z/OS DFSMSdss Advanced Services Return Codes from LOCATE.

IRR62076I  Parameter error. Text beginning with ‘text’ contains an undefined keyword.

Explanation: The listed text is not a parameter defined to the utility. The only parameter for IRRUT200 is ACTIVATE. Abbreviations are not accepted.

System action: Utility processing stops with RC12 (X'C').

System Programmer Response: Check the PARM field of the EXEC statement in the JCL.

RACF block update command (BLKUPD) messages

IRR63001I  Invalid command.

Explanation: One of the following situations occurred:

- The command is unknown.
- The command is a subcommand of READ and was entered without first entering the READ command.
- The command is a subcommand of READ or DISPLAY that attempts to update the RACF database, but UPDATE was not specified on the READ command.
- A READ (or DISPLAY) is in progress but the command entered is not a subcommand of READ (or DISPLAY).

System action: The command is ignored.

Programmer response: Enter another command.

IRR63002I  Offset is offset

Explanation: The search argument specified on the FIND command was located at the hexadecimal value xxx in the specified NEW or OLD block.

Programmer response: Enter another command, if you want.

IRR63003I  String not found.

Explanation: The search argument in the FIND command was not located in the specified NEW or OLD block.
Problem Determination: To view the contents of the NEW or OLD block, use the LIST or FORMAT command.

IRR63004I  REPLACE complete.
Explanation: The operation requested by the REP command is completed.
Programmer response: Enter another command.

IRR63005I  VERIFY failed. REPLACE not done.
Explanation: The string specified in the VER keyword of the REP subcommand was not found at the given offset, or the string extended beyond the end of the block.
System action: The string was not replaced. The command is ignored.
Programmer response: Enter another command.

Problem Determination: To view the contents of the NEW block, use the LIST or FORMAT command.

IRR63006I  READ ended. Block not saved.
Explanation: The function initiated by the READ command is ended and nothing is saved in response to the END command.
System action: The block was not written back to the RACF database because either NOSAVE was specified, or no changes were made to the block, or UPDATE was not specified on the READ command.
Programmer response: Enter a READ, LOCATE, or END command.

IRR63007I  UPDATE causes block overflow. NO changes made.
Explanation: The REP, or CHANGE and INSERT (under DISPLAY) operation is ignored because the modified block would be greater than 4096 bytes.
System action: The command is ignored.
Programmer response: Enter another command.
Problem Determination: To view the contents of the NEW block, use the LIST or FORMAT command.

IRR63008I  Old block recopied into new block.
Explanation: The REREAD subcommand of READ is complete. The NEW block is the same as the OLD block.
Programmer response: Enter another command.

IRR63009I  DISPLAY ended. Changes saved.
Explanation: The DISPLAY function is ended and the updates saved. The block may be changed further by subcommands of READ. The END SAVE subcommand of READ updates the RACF database with this block.
Programmer response: Enter another command.

IRR63010I  DISPLAY ended. Changes not saved.
Explanation: The DISPLAY function has ended without saving the changes made in response to the END (with NOSAVE) command, or because UPDATE was not specified on the READ command.
Programmer response: Enter a subcommand of READ.

Problem Determination: Record message number and RBA of READ command. Get a dump of the area you are trying to DISPLAY and check the data of the entry that had the error. Contact your IBM support center.

IRR63011I  Invalid data in index block. DISPLAY ended.
Explanation: The entry identifier or the length in the index is not correct.
System action: The DISPLAY function is ended and any changes made are not saved.
Programmer response: To correct the entry, use the LIST and REP subcommands of READ. Enter the DISPLAY subcommand again.

Problem Determination: To view the contents of the NEW block, use the LIST or FORMAT command.

IRR63012I  Block is not a valid index block.
Explanation: The block that is the object of a FORMAT or DISPLAY command is not a valid index block. The following tests are made for a valid index block:
- The first index block identifier (offset 00) must be X'8A'.
- The second index block identifier (offset 03) must be X'4E'.
- The displacement to free space must be greater than the displacement to the last entry.
- The displacement to free space must be less than 4096.
- The last byte before free space (the end of block delimiter) must be X'0C'.
- The entry identifier for all entries must be X'21' or X'22', except for the identifier of the last entry in a level 01 block, which must be X'20'.
- The lengths of all entries must be correct.
- The pointer section identifier—also called the E(P) byte—of each entry must be X'62' or X'66'.
System action: The command is ignored.
**Programmer response:** Make sure the RBA specified on the READ command is that of an index block. Use the LIST and REP subcommands of READ to fix the index block.

**Problem Determination:** Record message number and RBA of READ command. Get a dump of the area you are trying to DISPLAY or FORMAT and check the data of the index that had the error. Contact your IBM support center.

---

**IRR63013I**  READ ended. Block saved.

**Explanation:** The function initiated by the READ command is ended.

**System action:** The modified block is saved in the RACF database.

**Programmer response:** Enter a READ, LOCATE, or END command.

---

**IRR63014I**  Record not found.

**Explanation:** The RBA (relative byte address) specified on a READ command is not within the extents of the RACF database.

**System action:** The command is ignored.

**Programmer response:** Enter another READ command for a block within the RACF database.

---

**IRR63015I**  Open failed for DD SYSRACF.

**Explanation:** The BLKUPD command cannot open the RACF database defined by the SYSRACF DD statement.

**System action:** The BLKUPD command is ended.

**Programmer response:** Allocate the RACF database to DD SYSRACF and try again.

**Problem Determination:** Find out if the DD SYSRACF is already allocated to a data set.

---

**IRR63016I**  I/O error - jji, sss, ddd, devtyp, ddn, oper, err, xxxx, acc

**Explanation:** The BLKUPD command encountered a permanent I/O error while processing on device ddd.

**System action:** Command processing ends with a return code 12.

**Programmer response:** Examine the text of the message displayed on the terminal and match the error with codes in “Problem Determination.”

**Problem Determination:** In the message text, the error analysis information provided by the SYNAF data management macro instruction issued by the SYNAF routine was:

- **jjj**  Job name
- **sss**  Step name
- **ddd**  Unit address of the device
- **devtyp**  Device type
- **ddn**  Data definition name
- **oper**  Operation attempted
- **err**  Error description
- **xxxx**  Last seek address or block count
- **acc**  Access method

**IRR63017I**  Entry not found. Logical level 1 follows.

**Explanation:** The entry specified in a LOCATE command cannot be found. The level 1 block that ought to contain the specified entry is displayed.

**Programmer response:** Enter a READ, LOCATE, or END command. To add the entry to the block, use the DISPLAY subcommand of READ.

**Problem Determination:** To view the contents of the index block, use the LIST or FORMAT command.

---

**IRR63018I**  Index block chain for entry is broken.

**Explanation:** A block in the chain for a LOCATE command search is not a valid index block. The following tests are made for a valid index block:

- The same tests are made as shown for message IRR63012I.
- The RBA (relative byte address) for the next byte on the chain must be nonzero, with the two high-order bytes zero, and represent an address on a 4K boundary within the extent of the RACF database.
- The level of the block must be below the level of the previous block on the chain.

**System action:** The block is dumped in hexadecimal.

**Programmer response:** Correct the block in error by using the READ command and its subcommands.

**Problem Determination:** Run the IRRUT200 utility against the RACF database to find the troubled area.

---

**IRR63019I**  Error in sequence set. Index block at RBA rba.

**Explanation:** The sequence set block at the specified RBA (relative byte address) contains an error. The following tests are made for a valid block:

- The block must be in collating sequence with the previous block on the sequence set.
- The first index block identifier (offset 00) must be X'8A'.
- The second index block identifier (offset 03) must be X'4E'.

---
The displacement to free space must be greater than the displacement to the last entry.

The displacement to free space must be less than 4096.

The last byte before free space (the end of block delimiter) must be X'0C'.

The entry identifier of the last entry in the block must be X'20'.

The entry identifier for all other entries must be X'21' or X'22'.

All entries must have correct lengths and pointer section identifiers of X'62' or X'66'.

The block must be a level 01 block.

The RBA (relative byte address) for the next byte in the sequence set must be nonzero, with the two high-order bytes zero, represent an address on a 4K boundary within the extent of the RACF database, and be not more than 4 bytes long.

**System action:** The block is dumped in hexadecimal.

**Programmer response:** Correct the block in error by using the READ command and its subcommands.

**Problem Determination:** Examine the hexadecimal dump of the index block. Run the IRRUT200 utility against the RACF database to find the index problem.

---

**IRR63020I** Entry not found. DISPLAY ended.

**Explanation:** The DISPLAY command specified an entry that cannot be found in the index block.

**System action:** The command is ignored.

**Programmer response:** Reenter the DISPLAY command with an existing entry.

---

**IRR63021I** BLKUPD ended due to error- Unable to establish ESTAE.

**Explanation:** The BLKUPD command ended because of a system error. An ESTAE recovery environment cannot be established.

**System action:** Command processing ends with a return code of 12.

**Programmer response:** Enter the BLKUPD command again. If the problem persists, ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

**Problem Determination:** Examine system abend code and return code to determine the cause of the ESTAE setup failure.

---

**IRR63022I** Command not processed due to error+

**Explanation:** The TSO/E service routine indicated in the message failed with a return code of xx.

**System action:** Command processing ends with a return code of 12.

**Programmer response:** See the documentation containing the service routine for an explanation.

**Problem Determination:** For an explanation of the TSO/E service routines return codes, see z/OS TSO/E Programming Services. For the order number of the document you need, see z/OS TSO/E General Information.

---

**IRR63023I** Key length error+ Compression count plus key length must be from 1 to 255 characters.

**Explanation:** After processing a CHANGE or INSERT command, the compression count plus the key length of the new entry is less than 1 or greater than 255.

**System action:** The command is ignored.

**Programmer response:** Adjust the length or compression count so that the sum is 255 or less. Enter the command again.

**Problem Determination:** To view the contents of the index block, use the LIST or FORMAT command.

---

**IRR63024I** Invalid ICB. LOCATE ended.

**Explanation:** The LOCATE command found the ICB in the RACF database contains incorrect data. The sequence set RBA or the RBA of the first index block in the ICB is zero or not on a 4K boundary.

**System action:** The LOCATE command is ignored.

**Programmer response:** Correct the ICB by using the READ command and its subcommands. Check that the database used is the correct RACF database.

**Problem Determination:** Run the IRRUT200 utility against the RACF database to find the error.

---

**IRR63025I** Entry found.

**Explanation:** The entry requested by the LOCATE command was found with a sequence set search.

**System action:** The index block containing the entry is displayed.

**Programmer response:** Enter another command.
IRR63032I  Segment not defined in templates.
Explanation:  The segment name specified does not match any of the segments defined in the templates.
System action:  Command fails.
Programmer response:  Check the segment name that was specified as the SEGMENT parameter. Check to make sure that the templates on the database are not downlevel. At IPL, check for message ICH579E in the system log. Run IRRMIN00 PARM=UPDATE to correct the problem.

IRR63033I  Base segment cannot be specified.
Explanation:  The segment name of BASE specified on the command is incorrect. Only the RBA of the BASE segment can be updated.
System action:  Command fails.
Programmer response:  Check the segment name that was specified as the SEGMENT parameter.

IRR63034I  Segment already exists.
Explanation:  The segment name specified on the INSERT command already is defined to the current entry.
System action:  Command fails.
Programmer response:  Check the segment name that was specified as the SEGMENT parameter.

IRR63035I  Storage allocation failed.
Explanation:  The GETMAIN of storage for this module failed.
System action:  Processing ends with a return code of 12.
Programmer response:  Try the command again. If the same error occurs, check for a problem with storage management. Should storage management be fine, record this error, and call your IBM support center.
Problem Determination:  Examine the abend and return code from GETMAIN. See the proper documentation for details about failure codes.

IRR63036I  The first index entry has been deleted.
The rest of the index block may need to be updated.
Explanation:  The programmer just deleted the first index entry of an index block.
Programmer response:  Check the rest of the index entries for front-end compression. If they were compressed they might need to be decompressed to avoid errors in the index block. Also check that the index entries are still in collating sequence.
Problem Determination:  Use the FORMAT command to view the NEW block to analyze the index block that has been updated.

IRR63037I  The first index entry has been changed.
The rest of the index block may need to be updated.
Explanation:  The programmer just changed the first index entry of an index block.
Programmer response:  Check the rest of the index entries for front-end compression. If they were compressed they might need to be decompressed to avoid errors in the index block. Also check that the index entries are still in collating sequence.
Problem Determination:  Use the FORMAT command to view the NEW block to analyze the index block that has been updated.

IRR63038I  The first index entry has been inserted.
The rest of the index block may need to be updated.
Explanation:  The programmer just inserted a new first index entry into the current index block.
Programmer response:  Check the rest of the index entries for front-end compression. If they were compressed they might need to be decompressed to avoid errors in the index block. Also check that the index entries are still in collating sequence.
Problem Determination:  Use the FORMAT command to view the NEW block to analyze the index block that has been updated.

IRR63039I  Segment does not exist.
Explanation:  The segment name specified on the SEGMENT keyword of the CHANGE or DELETE commands is not defined to the current index entry.
System action:  Command fails.
Programmer response:  DISPLAY the index entry again and examine it to be sure that it is the correct entry. If the segment you want to update is not there, use the INSERT command to insert it.
Problem Determination:  Use the DISPLAY command to view the index entry and its segments.

IRR63040I  Input data set is invalid. Processing terminated.
Explanation:  The data set specified on the BLKUPD command is not a valid format RACF data set.
System action:  The BLKUPD command ends with a return code of 12.
Programmer response:  Check the data set name. Be sure the data set block size is 4096. Call your IBM support center with this message number and a listing
of the data set you are trying to use with BLKUPD.

IRR63041I  Could not read the ICB.

Explanation: The RACF data set specified on the
BLKUPD command cannot be validated for its format
because the ICB cannot be read.

System action: BLKUPD command processing ends
with a return code of 12.

Programmer response: Check the data set name. Be
sure the data set block size is 4096.

Problem Determination: Run the IRRUT200 utility to
validate the RACF data set and to point out any
discrepancies. Call your IBM support center with this
message number and a listing of the data set you are
trying to work with.

IRR63042I  This is not a level 1 index block, no
segment information is available.

Explanation: The index block that was read in by the
READ command is not a level-1 index block. The
SEGMENT keyword of the DISPLAY command and its
subcommands is only valid for level-1 index blocks.

System action: The subcommand of DISPLAY
(CHANGE, INSERT, or DELETE) fails, and utility
processing continues.

System programmer response: End processing of the
DISPLAY command and perform a FORMAT
subcommand under READ. Determine the level of the
index block being listed by the output of the FORMAT
subcommand. Reassess which level-1 index block RBA
you intended to work with, END the READ command,
and issue the READ command with the RBA of the
level-1 index block.

IRR63043I  The ICB indicates the input data set is
not a Restructured Database. The ICB
may be corrupt. Processing Continues.

Explanation: The ICBDIFMT field of the ICB, for the
RACF database specified on the BLKUPD command,
indicates that the database supplied is not a
restructured RACF database.

System action: Utility processing continues.

System programmer response: Use the
BLKUPD/READ/LIST ALL command to examine the
ICB and assess the extent of the damage to the ICB. If
the ICB is extensively damaged, call your IBM support
center with this message number and a listing of the
data set you are trying to update.

IRR63044I  BLKUPD UPDATE processing is not
permitted while the system is in
read-only mode.

Explanation: A BLKUPD command was entered
requesting UPDATE of the RACF data set. The system
is currently in read-only mode and updating of the
RACF data set is not allowed.

System action: The BLKUPD command is not
processed.

System programmer response: To make a change to
the RACF data set, you can do one of the following
tasks:
• Issue BLKUPD from another system that is not in
read-only mode.
• Issue RVARY DATASHARE to change the mode of
all systems to data sharing mode and reissue the
BLKUPD READ UPDATE.
• Issue RVARY NODATASHARE to change the mode
of all systems to non-data sharing mode and reissue
the BLKUPD READ UPDATE.

IRR63045I  A coupling facility related error has
occurred. BLKUPD processing has
ended abnormally.

Explanation: An error occurred when accessing the
coupling facility.

System action: BLKUPD processing ends abnormally.

System programmer response: Check the information
specified in IRRX016I, which is issued to the system
console. Changes requested by BLKUPD might have
taken effect. Verify these changes after the coupling
facility related error has been corrected. Reissue
BLKUPD again, as necessary.

IRR63046I  The BLKUPD command does not
support the keyword keyword.

Explanation: An undefined keyword was encountered
during processing of the BLKUPD command.

System action: The command is not processed.

User response: Check the command syntax and issue
the command again.

Operator response: None.
RACF database split/merge utility (IRRUT400) messages

**IRR65000I** Invalid input to message writing routine attempting to write message number message-number.

**Explanation:** This is an error internal to the utility. The specified message-number was not found.

**System action:** System processing continues.

**Problem Determination:** Record the specified message number and contact your IBM support center.

**IRR65001I** Element number number of range table is out of sequence.

**Explanation:** The indicated range table entry is out of collating sequence.

**System action:** Utility processing stops.

**System programmer response:** Ensure that the range table was assembled and link-edited correctly. For information about using a range table, see z/OS Security Server RACF System Programmer’s Guide.

**Problem Determination:** Verify that each entry in the range table appears with its keys in ascending order.

**IRR65002I** Unable to load module table-name to be used as range table.

**Explanation:** The load module named in the TABLE keyword cannot be loaded into storage.

**System action:** Utility processing stops.

**System programmer response:** A STEPLIB DD statement might be missing.

**Problem Determination:** Check for other errors related to the disk pack on which the database resides.

**IRR65003I** error-type on ddname attempting a request of block at RBA rba.

**Explanation:** The indicated error occurred while attempting a BDAM read (READ), BDAM write (WRITE), or BSAM write (LOAD).

**System action:** The ddname of the file on which the error occurred is listed, along with the RBA (relative byte address) of the byte being accessed.

**System programmer response:** To recover from the problem, ensure that the DD statement is correct.

**Problem Determination:** Check for other errors related to the disk pack on which the database resides.

**IRR65004I** Range table contains no elements or first element string is not binary zeros.

**Explanation:** The first fullword of the range table is binary zeros, indicating no elements in the table, or the string portion of the first element is not binary zeros, as is required.

**System action:** Utility processing stops.

**Programmer response:** Ensure that the range table was assembled and link-edited correctly. For information about using a range table, see z/OS Security Server RACF System Programmer’s Guide.

**Problem Determination:** Record the specified message number and contact your IBM support center.

**IRR65005I** RACF data set full on ddname.

**Explanation:** Space has been exhausted on the specified output RACF database.

**System action:** Utility processing stops.

**System programmer response:** Increase the size of the output database.

**Problem Determination:** This message is accompanied by message number IRR65018I, which can be used to determine how much data has already been processed.

**IRR65006I** Unable to open dsname, ddname.

**Explanation:** If the database is for input, the utility stops processing. If the database is for output, only processing to that database ends.

**System action:** Utility processing stops.

**System programmer response:** To recover from the problem, ensure that the DD statement is correct.

**Problem Determination:** Check for other errors related to the disk pack on which the database resides.

**IRR65007I** Information retrieval for ddname failed with error code code.

**Explanation:** RACF issued a dynamic allocation request (SVC 99) for information about the ddname indicated in the message. However, the return code from dynamic allocation was unexpected.

**System programmer response:** See “Problem Determination.”

**Problem Determination:** Check the return code from the SVC 99 in z/OS MVS Programming: Authorized Assembler Services Guide.

**IRR65008I** dsname successfully opened for open-type on ddname.

**Explanation:** The named database has been successfully opened (BSAM open for INITIALIZATION or BDAM open for PROCESSING) with the given ddname.

**System action:** Utility processing continues normally.
IRR65009I  No input DD statements found - Processing terminated.

Explanation: The utility cannot perform without at least one input RACF database.

System programmer response: Ensure that at least one DD statement has been allocated.

Problem Determination: Check the JCL DD statements to verify this.

IRR65010I  LOCK function requested, ddname already locked.

Explanation: To prevent updates to the database indicated by ddname, the LOCK function is requested. If the database was not located previously, it is locked at this time.

System action: Utility processing continues.

IRR65011I  Lock recovery disposition successful for ddname.

Explanation: This message reports the results of the attempt to turn the extend bit OFF in the ICB for the listed ddname. If lock recovery is not successful, the bit remains ON in that ICB. If lock recovery is successful, the bit has been turned OFF.

System action: Utility processing continues.

IRR65012I  profile-name in class class-name from ddname is duplicate of same name from ddname.

Explanation: The named profile cannot be copied to an output database because it has the same name as a profile already copied from another input database. Either the profile is in a class other than DATASET or the NODUPDATASETS option is in effect.

System action: Utility processing stops for the named profile.

Problem Determination: Check the PARM field of the EXEC statement for this utility. For duplicate names, option DUPDATASETS must be in effect. Also, check to see what class the profile is actually in. The return code is the highest one found during all processing.

IRR65013I  Index entry entry-name on ddname points to a tape volume set of which it is not a member.

Explanation: The index entry indicated by entry-name does not appear in the volume list of the profile for the tape volume set to which it points.

System action: The index entry is not copied to an output database. The tape volume set is copied if no other errors exist.

System programmer response: See “Problem Determination.”

Problem Determination: Ensure that the index entry and database specified by DD statement are both correct.

IRR65014I  A tape volume set from ddname is inconsistent with the range table, member names follow: member-name member-name ...

Explanation: The range table specified with the TABLE keyword does not designate all of the members of the set to be copied to the same output database. The member names listed are not prefixed by the characters TAPEVOL-, but the prefix was used when interrogating the range table.

System action: The tape volume set is not copied to output.

IRR65015I  A tape volume set from ddname1 contains a duplicate of entry-name from ddname2, member names follow: member-name member-name ...

Explanation: Two tape volume sets contain the same name in their volume lists. Therefore, only one of the sets can be copied to the output database.

System action: The entire tape volume set whose members are listed is not copied to output.

IRR65016I  abend-code abend during utility processing.

Explanation: The specified abnormal termination occurred during the execution of the utility.

System action: Utility processing stops.

System programmer response: See “Problem Determination.”

Problem Determination: Use the indicated abend code and any previous messages issued by this utility, to determine the appropriate action. See your MVS system codes documentation for more information about the abend indicated in the message.

IRR65017I  Unable to establish recovery environment. Processing terminated.

Explanation: Processing stops because adequate recovery cannot be provided.

System action: Utility processing stops.

System programmer response: Ensure that RACF and the operating system are properly installed. If they are, contact your IBM support center.
IRR65018I  Output processing to ddname terminated while processing entry entry-name.

Explanation: Because of an error identified by the message immediately preceding this message on the output, no further processing of the data set indicated by ddname is attempted. The data set should not be used as a RACF database.

System action: Utility processing stops.

Problem Determination: Use the information given by both this and the preceding message to determine the proper corrective action.

IRR65019I  Output processing to ddname terminated due to failure during data set initialization.

System action: Utility processing stops.

Explanation: An error occurred while performing information retrieval, opening, writing a block, or using BSAM to write empty blocks. This message follows messages IRR65003, IRR65006, and IRR65007. See the previous message description for more information.

System action: Processing to the database stops.

System programmer response: To recover from the problem, ensure that the DD statement is correct.

IRR65020I  Specified options: parm

Explanation: The parameters specified by the user on the EXEC statement are listed.

System action: Utility processing continues normally.

IRR65021I  Parameter error. Text beginning with 'text' contains an undefined keyword.

Explanation: The listed text does not start with a keyword defined to the utility.

System action: Utility processing stops.

System programmer response: Check the PARM field of the EXEC statement in the JCL.

Problem Determination: Ensure that any abbreviations for keywords contain enough significant characters to make the abbreviation uniquely identifiable to the utility.

IRR65022I  Parameter error. Keyword 'keyword' is ambiguous.

Explanation: The utility has more than one keyword with the character string indicated by keyword.

System action: Utility processing stops.

System programmer response: Ensure that abbreviations for keywords contain enough significant characters to make the abbreviation uniquely identifiable to the utility.

IRR65023I  Parameter error. Text beginning with 'text' is redundant or contradictory to a previous specification.

Explanation: Either the keyword contained in the text or its opposite form was specified previously. The utility uses the first specification of the keyword.

System action: Utility processing stops.

System programmer response: Ensure that abbreviations for keywords contain enough significant characters to make the abbreviation uniquely identifiable to the utility.

Problem Determination: For a complete description of all parameters supported by this utility, see z/OS Security Server RACF System Programmer’s Guide.

IRR65024I  Parameter error. Keyword 'keyword(value)' contains an unacceptable value.

Explanation: The value specified is not acceptable when associated with the keyword listed.

System action: Utility processing stops.

System programmer response: See “Problem Determination.”

Problem Determination: For a complete description of all parameters supported by this utility, see z/OS Security Server RACF System Programmer’s Guide.

IRR65025I  Options in effect: options

Explanation: All options, including default options, in effect for the execution of this utility are listed.

System action: Processing continues normally.

IRR65026I  Options in Effect: UNLOCKINPUT

Explanation: UNLOCKINPUT is the only option specified for this execution of the utility.

System action: The utility unlocks the input databases. The utility does not copy the databases.

IRR65027I  UNLOCKINPUT is the only option allowed. Processing terminated.

Explanation: More than one option was specified. UNLOCKINPUT must be the only option requested for execution.

System action: Utility processing stops.

System programmer response: Specify the UNLOCKINPUT parameter without any other option.
IRR65028I  UNLOCK function requested, ddname already unlocked.
Explanation: The database indicated by ddname was unlocked before this attempt to unlock it.
System action: Processing continues normally.

IRR65029I  UNLOCK function requested, ddname now unlocked.
Explanation: The database indicated by ddname has been unlocked and is now ready for updates.
System action: Processing continues normally.

IRR65030I  UNLOCK was not successful for ddname
Explanation: An error occurred while attempting to unlock an input database. One of the following situations has occurred:
- The database indicated by ddname was not found.
- Unable to open ddname.
- Retrieval error for ddname.
- Permanent I/O error.
System action: The database indicated by ddname was not unlocked. Processing stops.
System programmer response: To recover from the problem, do the following tasks:
- Ensure that the DD statement is specified correctly.
- Check if ddname is already allocated.
- Check if there were other error messages previous to this one.
Problem Determination: If other error messages preceded this one, refer to those message explanations to determine the cause of the problem.

IRR65031I  No locking parameter was specified. Processing will terminate after the following message.
Explanation: Without a locking parameter, the utility cannot continue processing.
System action: Utility processing stops after the following message.
System programmer response: See the following message.

IRR65032I  One of the following parameters is required: LOCKINPUT, NOLOCKINPUT, or UNLOCKINPUT.
Explanation: Without a locking parameter, the utility cannot continue processing.
System action: Utility processing stops.
System programmer response: Specify a locking parameter and invoke the utility again.

IRR65033I  Incorrect ICB found on ddname. Processing will terminate.
Explanation: The ICB related to the RACF database indicated by the ddname in the message cannot be used by the utility.
System action: Utility processing stops.
System programmer response: Check that you have specified the correct ddname and that it represents the RACF database you want to use. If it is, and the RACF database was not previously formatted using this utility with the PARM='NEW' specification, rerun the utility with PARM='NEW'.
Problem Determination: The validity check that caused the failure can result from an incorrect ICB value for the number of templates or BAMs, or an incorrect RBA (relative byte address). List the contents of the data set defined by the SYSRACF DD statement to determine the cause of the problem.

IRR65034I  Incorrect blocksize found on ddname, IRRUT400 expects a blocksize of 4096. Processing will terminate.
Explanation: The DCB for the input ddname data set indicates a block size other than 4096. IRRUT400 only processes a data set with LRECL and BLOCKSIZE equal to 4096.
System action: Utility processing stops.
System programmer response: Ensure that the data set name specified on the ddname DD statement has a block size of 4096.

IRR65035I  Database LOCKINPUT/UNLOCKINPUT parameters are not permitted while the system is in read-only mode.
Explanation: LOCKINPUT/UNLOCKINPUT attempts to update the extend bit in the ICB. However, no database updates can be made while the system is in read-only mode.
System action: Utility processing stops.
System programmer response: You can do one of the following tasks:
- Run IRRUT400 with a parameter of LOCKINPUT/UNLOCKINPUT from another system that is not in read-only mode.
- Issue RVARY DATASHARE to change the mode of all systems to data sharing mode and rerun the job.
- Issue RVARY NODATASHARE to change the mode of all systems to non-data sharing mode and rerun the job.
A coupling facility related error occurred during database LOCKINPUT/UNLOCKINPUT processing. Utility processing has ended abnormally.

Explanation: An error occurred when accessing the coupling facility.

System action: IRRUT400 processing ends abnormally.

System programmer response: Check the SYSPRINT. Also, check the information specified in message IRRX016I, which is issued to the system console.

If the error occurred during the locking of the data sets, IRRUT400 processing has not completed. If any data sets have been locked, you should either:
- Rerun the job from the original system if it is still in data sharing mode. You should specify the UNLOCKINPUT parameter first, followed by the LOCKINPUT parameter.
- Rerun the job from another system in the RACF sysplex data sharing group, if that system is in data sharing mode. You should specify the UNLOCKINPUT parameter first, followed by the LOCKINPUT parameter.

If the error occurred during the unlocking of the data sets, you should either:
- Rerun the job from the original system if it is still in data sharing mode. You should specify the UNLOCKINPUT parameter.
- Rerun the job from another system in the RACF sysplex data sharing group, if that system is in data sharing mode. You should specify the UNLOCKINPUT parameter.

No valid ddname statement was found. Processing continues, but ignores this output database.

Explanation: This message appears for each output DD statement that was not found in your JCL.

System action: The IRRUT400 utility continues processing to identify inconsistencies between one or more input RACF databases. The range of profiles normally directed to the missing output DD statement are not written.

System programmer response:
- If the IRRUT400 utility ran without errors and you are running the utility to check for inconsistencies, this message is for your information only. No response is needed.
- If you meant to redistribute or copy one or more RACF databases, you must code an output DD statement (OUTDD1, OUTDD2, and so on) for every output RACF database. For more information about allocating output databases for this utility, see z/OS Security Server RACF System Programmer’s Guide.

ICB for an empty database found on ddname. The database will be ignored.

Explanation: The ICB from the RACF database identified by ddname was found to be valid, but the database contained no profiles.

System action: The database identified by ddname is ignored by the IRRUT400 utility and processing continues. If all databases contain valid ICBs but no profiles, a return code of 16 is returned and processing stops.

System programmer response: Check that you have specified the correct DDNAME and that it represents the RACF database you want to use.

Database ddname must be processed with a z/OS V1R5.0 or later level of IRRUT400. Processing stops.

Explanation: The templates on database ddname are at a z/OS V1R5.0 (FMID HRF7708) or later level and can only be processed with a version of the IRRUT400 utility that is that level or greater. The IRRUT400 version you are attempting to use is before z/OS V1R5.0.

System action: Utility processing stops.

System Programmer Response: Check that you have specified the correct ddname and that it represents the RACF database you want to use. If it is, then run IRRUT400 from the latest level of the z/OS V1R5.0 or later systems that are sharing the RACF database.

Output processing failed. ddname specifies an active RACF database on this system.

Explanation: The RACF database identified by ddname is an active primary or backup for this system. It cannot be overwritten while active.

System action: Processing ends with a return code of 16.

System Programmer Response: Correct the data set specified on the DD statement and run the utility again.

If you are attempting to synchronize the primary and backup data sets, see the section on copying your database in z/OS Security Server RACF System Programmer’s Guide.

Database copy (INDDnn to OUTDDnn) failed. Same data set specified for input and output.

Explanation: A copy of the RACF data set has been requested but an INDD and an OUTDD DD statement point to the same data set. IRRUT400 will not copy a data set over itself.
System action: Processing ends with a return code of 16 (X’10’)
System Programmer Response: Correct your DD statements to point to the correct data sets and run the IRRUT400 utility again

Internal reorganization of aliases utility (IRRIRA00) messages

IRR66000I Invalid input to message writing routine attempting to write message number message-number.
Explanation: This is an error internal to the utility. The specified message number was not found.
System action: System processing continues. Utility processing may or may not continue.
Programmer response: Record the specified message number and contact your IBM support center.

IRR66001I Unable to establish recovery environment. Processing ended.
Explanation: An estae environment cannot be established.
System action: Utility processing stops.
Programmer response: Report this problem to your system programmer.
System programmer response: Ensure that RACF and the operating system are properly installed. If they are, contact the IBM support center.

IRR66002I Unable to run IRRIRA00. RACF is not active.
Explanation: RACF is not installed on the system, or it is inactive.
System action: Utility processing stops.
Programmer response: Report this problem to your system programmer.
System programmer response: Ensure that RACF is properly installed, and is active on the system.

IRR66003I Unable to run IRRIRA00. Backup RACF database is partially inactive.
Explanation: The backup RACF database contains multiple data sets. Some data sets are currently active, and some inactive. The utility cannot create a valid backup database in this state.
System action: Utility processing stops.
Programmer response: Report this problem to your system programmer.
System programmer response: Issue RVARY to activate or inactivate all data sets in the backup RACF database and rerun the job.

IRR66004I RACF database cannot be updated. System is in read-only mode.
Explanation: IRRIRA00 must update the RACF database to change the current stage. However, no database updates can be made because the system is currently in read-only mode.
System action: Utility processing stops.
Programmer response: Run IRRIRA00 from another system that is not in read-only mode, or report the problem to your system programmer.
System programmer response: You can do one of the following tasks:
• Issue RVARY DATASHARE to change the mode of all systems to data sharing mode and rerun the job.
• Issue RVARY NODATASHARE to change the mode of all systems to non-data sharing mode and rerun the job.

IRR66005I A coupling facility related error occurred. Utility processing has ended abnormally.
Explanation: An error occurred when accessing the coupling facility.
System action: Utility processing stops.
Programmer response: Check the SYSPRINT for related error messages and report them to your system programmer. Run IRRIRA00 from another system in the data sharing group.
System programmer response: Check for related console and syslog messages and perform any actions associated with the responses for those messages.

IRR66006I Stage stage-number requested. Database already at requested stage.
Explanation: The RACF database was already at the stage specified by the stage parameter.
System action: Utility processing stops.
Programmer response: If you want to move the system to the next stage, correct the value of the stage parameter and run the job again.

IRR66007I Backup RACF database not converted to stage stage-number. It is not active.
Explanation: The RACF primary database was converted to the stage requested, but the backup RACF
database was not converted because it is not currently active.

System action: Utility processing continues.

Programmer response: Copy the primary RACF database to the backup before activating the backup database.

IRR66008I  abend-code  abend during utility processing.
Explanation: The specified abnormal termination occurred during the execution of the utility.
System action: Utility processing stops.
Programmer response: Use the indicated abend code and any previous messages issued to determine the appropriate action. Rerun the job after correcting the problem.

IRR66009I  Last entry processed successfully was entry-name in class class-name.
Explanation: Because of an error identified by a preceding message, no further processing of this database will be attempted.
System action: Utility processing stops.
Programmer response: Correct the error indicated by any previous messages issued and rerun the job.

IRR66010I  Parameter error. Unsupported stage value specified.
Explanation: The stage parameter specified a value that is not in the supported range.
System action: Utility processing stops.
Programmer response: Correct the stage parameter and run the job again.

IRR66011I  Parameter error. Undefined parameter specified.
Explanation: A parameter was specified that is not recognized by the utility.
System action: Utility processing stops.
Programmer response: Correct the specified parameter and run the job again.

IRR66012I  Parameter error. Converting from stage current-stage-number to stage specified-stage-number is not allowed.
Explanation: The utility cannot convert the database from its current stage to the stage specified by the stage parameter.
System action: Utility processing stops.

Programmer response: Correct the value specified for the stage parameter and run the job again.

IRR66013I  Parameter error. No closing parenthesis found.
Explanation: The utility did not find a closing parenthesis in the parameter specification.
System action: Utility processing stops.
Programmer response: Correct the parameter specification and run the job again.

IRR66014I  Parameter error. No stage value specified.
Explanation: The utility did not find a value specified for the stage parameter.
System action: Utility processing stops.
Programmer response: Specify a value for the stage parameter, or omit the parameter to display the current stage, and run the job again.

IRR66015I  Parameter error. Extraneous text follows stage parameter.
Explanation: The utility found unexpected text following the value specified for the stage parameter.
System action: Utility processing stops.
Programmer response: Correct the parameter specification and run the job again.

IRR66016I  Unexpected RACF manager return code [deleting | updating] entry entry-name in class class-name. Return code return-code. Reason code reason-code.
Explanation: While altering the RACF database, a return code was returned by the RACF manager indicating that an error was encountered.
System action: Utility processing stops.
Programmer response: Use the decimal return code and reason code to determine the cause of the problem. z/OS Security Server RACF Macros and Interfaces contains the ICHEINTY return and reason codes. Correct the problem and run the job again.

IRR66017I  The system is currently operating in stage stage-number.
Explanation: The RACF RCVT indicates that the system is currently operating in the stage indicated. This is a status message only.
System action: None.
Programmer response: If you want to move the
system to the next stage, rerun the utility with the stage
c parameter specified.

**IRR66018I**  Stage stage-number requested. Database
now at requested stage.

**Explanation:**  The RACF database was successfully
converted to the stage specified by the stage parameter.

**System action:**  None.

**IRR66019I**  Unable to open dsname.

**Explanation:**  The utility was unable to open the RACF
data set dsname to process the ICB.

**System action:**  Utility processing stops.

**Programmer response:**  Check for other errors related
to the DASD volume on which the data set resides,
correct the problem and rerun the job.

**IRR66020I**  [Allocation | Deallocation] for dsname
failed with error code code.

**Explanation:**  The utility issued a dynamic allocation
request (SVC 99) to allocate or deallocate the RACF
data set dsname. However, the return code from
dynamic allocation was unexpected.

**Programmer response:**  Check the return code from the
SVC 99 in z/OS MVS Authorized Assembler Services
Guide and correct the problem. If the error took place
during deallocation processing, the stage value may
already have been incremented. Rerun the job to check
or increment the stage value.

**IRR66021I**  Unexpected RACF manager return code
attempting to locate next entry after
entry entry-name in class class-name.
Return code return-code. Reason code
reason-code.

**Explanation:**  While reading the RACF database, a
return code was returned by the RACF manager
indicating that an error was encountered.

**System action:**  Utility processing stops.

**Programmer response:**  Use the decimal return code
and reason code to determine the cause of the problem.
\texttt{z/OS Security Server RACF Macros and Interfaces}
contains the ICHEINTY return and reason codes. Correct the
problem and run the job again.

**IRR66022I**  Unable to run IRRIRA00. Templates are
downlevel and do not support alias
index entry creation.

**Explanation:**  IRRIRA00 has detected that the level of
templates currently in use does not support the
creation of alias index entries.

**System action:**  Utility processing stops.
**RACF database unload utility (IRRDBU00) and RACF SMF data unload utility (IRRADU00) messages**

---

**IRR67000I** Incorrect input to message writing routine attempting to write message number message-number

**Explanation:** This is an error internal to the utility. The specified message number was not found.

**System action:** Utility processing continues.

**Problem Determination:** Record the specified message number and contact your IBM support center.

**IRR67001I** Unable to establish recovery environment. Processing terminated.

**Explanation:** An ESTAE environment cannot be established.

**System action:** Utility processing stops.

**System programmer response:** Ensure that RACF and the operating system are properly installed. If they are, report this message (including its message ID) to your IBM support center.

**Problem Determination:** See “System Programmer Response”.

---

**IRR67041I** utility-name UNSUCCESSFUL: CANNOT OPEN SYSPRINT.

**Explanation:** The sysprint DCB cannot be opened in order to enable messages to be printed.

**System action:** Utility processing stops.

**System programmer response:** Ensure that SYSPRINT has been allocated in the JCL.

**Problem Determination:** See “System Programmer Response”.

**Note:** This is a WTO with routing code 11.

---

**IRR67005I** RACF is not active.

**Explanation:** RACF is not installed on system or it is inactive.

**System action:** Utility processing stops.

**System programmer response:** Ensure that RACF is properly installed on system.

**Problem Determination:** Contact your IBM support center if this problem recurs.

---

**IRR67006I** RACF is not at appropriate release level.

**Explanation:** RACF is installed, but is not at least version 1.9.0.

**System action:** Utility processing stops.

---

**IRR67007I** The blocksize was taken from DD ddbname and the data set was closed.

**Explanation:** The block size was successfully read from the specified database.

**System action:** Utility processing continues.

---

**IRR67008I** The blocksize was taken from DD ddbname but an error occurred while closing the data set.

**Explanation:** The block size was successfully read from the specified data set, but this data set cannot be closed.

**System action:** Utility processing stops.

**Problem Determination:** This message is accompanied by messages issued by DFP. Follow the problem determination procedure for the DFP messages. These are contained in the MVS system messages document.

---

**IRR67010I** Specified option: option

**Explanation:** The parameter specified with the PARM= field in the EXEC statement is listed here. The parameters NOLOCKINPUT, LOCKINPUT, and UNLOCKINPUT can be abbreviated to a minimum of N,L, and U, respectively. If no option is specified, message IRR67021I is issued.

**System action:** Utility processing continues.

---

**IRR67011I** Parameter error. Text beginning with ‘text.’ contains an undefined keyword.

**Explanation:** An incorrect parameter was passed to the utility.

**System action:** Utility processing stops.

**System programmer response:** Ensure that only one of the following was specified: NOLOCKINPUT, LOCKINPUT, or UNLOCKINPUT.

**Problem Determination:** Check the PARM= field of the EXEC statement.

---

**IRR67012I** Parameter error. Text beginning with ‘text.’ is longer than valid keywords.

**Explanation:** An incorrect parameter was passed to the utility.
**System action:** Utility processing stops.

**System programmer response:** Ensure that only one of the following was specified: NOLOCKINPUT, LOCKINPUT, or UNLOCKINPUT.

**Problem Determination:** Check the PARM= field of the EXEC statement.

---

**IRR67013I**  
Option in effect: *option*

**Explanation:** The full text of the option that the utility processes (based on the PARM operand of the EXEC statement) is displayed here.

**System action:** Utility processing continues.

---

**IRR67016I**  
RACF unable to build an ACEE.  
RACINIT return code is *return-code*.

**Explanation:** The accessor environment element (ACEE) cannot be built for either the input or output RACF database.

**System action:** Utility processing stops.

**System programmer response:** Be sure that RACF is properly installed on system.

**Problem Determination:** Record RACINIT return code and this message ID. Contact your IBM support center.

---

**IRR67020I**  
Parameter error. Text ‘text’ is incorrect. Only one parameter may be specified.

**Explanation:** More than one parameter was passed to the utility on the EXEC statement.

**System action:** Utility processing stops.

**System programmer response:** Ensure that only one of the following was specified: NOLOCKINPUT, LOCKINPUT, or UNLOCKINPUT.

**Problem Determination:** Check the PARM= field in the EXEC statement.

---

**IRR67021I**  
No parameter specified. One of the following is required: LOCKINPUT, NOLOCKINPUT, or UNLOCKINPUT.

**Explanation:** No parameters were passed to the utility.

**System action:** Utility processing stops.

**System programmer response:** Ensure that only one of the following is specified: NOLOCKINPUT, LOCKINPUT, or UNLOCKINPUT.

**Problem Determination:** Check the PARM= field in the EXEC statement.

---

**IRR67060I**  
*** Profile processing not started ***

**Explanation:** No database processing was attempted because of a previous failure in setting up the utility.

**System action:** Utility processing stops.

**System programmer response:** Ensure that the proper initializations were made before executing the utility. Rerun the utility after correcting errors identified in previous messages.

**Problem Determination:** Use the messages displayed before this one to help determine what the specific problem is.

---

**IRR67090I**  
Unexpected RACF manager return code while reading the data base. The next message contains diagnostic information.

**Explanation:** While attempting to read the RACF database, a return code was returned by RACF indicating an error during the READ operation.

**System action:** Utility processing stops.

**System programmer response:** The next message, IRR67092I, contains the return code, the reason code, and the entry that was being processed. Use this information and information about ICHEINTY return codes from [z/OS Security Server RACF Macros and Interfaces](https://www.ibm.com/support/knowledgecenter/SS7370_13.1.0/rac_zos_security_server_racf_macros_and_interfaces) to determine the proper action.

---

**IRR67091I**  
Return code: *return-code* reason code: *reason-code* entry name: *entry-name*.

**Explanation:** This message is issued after IRR67090I. This message contains the return code, reason code, and entry name that were returned from the failing request. A blank entry name indicates that the utility was processing the first entry in the profile type.

**System action:** Utility processing stops.

**Problem Determination:** Use the return code and reason code to determine the cause of the problem.

---

**IRR67092I**  
Processing *profile-type* profiles.

**Explanation:** This is an informational message identifying the type of profiles that the utility is now processing.

**System action:** Processing continues.

---

**IRR67120I**  
*abend-code* abend during utility processing. Reason code *reason-code*.

**Explanation:** A system abend occurred during utility processing.
System action: Utility processing continues with recovery procedures.

Problem Determination: For more information about the indicated abend, see z/OS MVS System Codes.

IRR67121I The module in control at time of abend was module-name.

Explanation: The internal module that was in control at the time of the abend is listed here for debugging purposes.

System action: Utility processing continues with recovery procedures.

Problem Determination: This message is accompanied by message IRR67120I. If the problem recurs after following the problem determination for the above message number, then record all information provided by these two messages and contact your IBM support center.

IRR67122I *** Utility ESTAE error routine in control. ***

Explanation: The recovery procedure for the utility is now processing.

System action: Recovery processing begins.

IRR67123I Profile processing DID finish before the abend. Output should be complete.

Explanation: The recovery routine has determined that the abend specified in message IRR67120I occurred after all profiles had been processed. The output file should be complete. The abend must have occurred during resource cleanup.

System action: Recovery processing continues.

Problem Determination: Verify that the utility completed, using the IRRUT200 verification utility.

IRR67124I Profile processing DID NOT finish before the abend. Output is NOT complete.

Explanation: The recovery routine has determined that the abend specified in message IRR67120I occurred before the utility completed.

System action: Recovery processing continues.

System programmer response: The output file was too small. Allocate a bigger output file and rerun the utility.

IRR67125I Utility ESTAE error routine will now attempt clean-up processing.

Explanation: An attempt is made to free all main storage that was used by the utility.

Note: If message IRR67124I was issued before this message, and you specified the LOCKINPUT parameter to lock the databases, the databases remain unlocked unless they were already locked before the utility was invoked.

IRR67150I Processing count RACF data set(s).

Explanation: The database utility expects to process the indicated number of RACF data sets. This number is taken from the system data set name table (ICHRDSNT).

System action: Processing continues normally.

IRR67151I LOCKINPUT parameter specified. DD ddname is now locked.

Explanation: The LOCKINPUT parameter was specified in the input specifications for the utility. The RACF database is locked. Others cannot write to the RACF database until the database is unlocked. To unlock the database, use the IRRUT400 or IRRDBU00 utility with the UNLOCKINPUT parameter specified.

System action: Processing continues normally.

IRR67152I LOCKINPUT parameter specified. DD ddname was already locked. Processing continues with this DDNAME.

Explanation: The LOCKINPUT parameter was specified in the input specifications for the utility, but the specified RACF database was already locked. Others cannot write to the RACF database until the database is unlocked. To unlock the database, use the IRRUT400 or IRRDBU00 utility with the UNLOCKINPUT parameter specified.

System action: Processing continues normally.

IRR67153I Unexpected DD statement ddname found.

Explanation: You specified more DD statements than the RACF utility expected.

System action: Processing stops.

System programmer response: Ensure that the number of INDDx statements is the same as indicated by message IRR67150I.
IRR67154I  Blocksize is incorrect for data-set-name on volume volume.

Explanation: The block size specified for the indicated data on the indicated volume is incorrect.

System action: Processing stops.

System programmer response: Omit the BLKSIZE parameter on the DD statement, or specify the correct value for the indicated RACF database.

---

IRR67155I  INDD1 is neither a primary nor backup data set. No other input data set can be a primary or backup data set.

Explanation: The utility is processing a database that is not being used by RACF as either a primary or backup database.

System action: Processing continues normally.

System programmer response: Make sure that any updates to the primary or backup database are incorporated in the database that is produced by the utility.

---

IRR67156I  DD ddname specifies a primary or backup data set, but a non-primary or non-backup data set was expected.

Explanation: The DD statement for INDD1 specifies a nonprimary or nonbackup data set. Therefore, the utility expects all data sets to be nonprimary or nonbackup data sets. However, the ddname indicated in the message specifies a primary or backup data set.

System action: The utility stops processing.

System programmer response: Correct the DD statements and rerun the job.

---

IRR67157I  DD ddname is not a primary data set. The following message shows the expected primary data set.

Explanation: The DD statement for INDD1 specifies a primary data set. Therefore, the utility expects all data sets to be primary data sets. However, the ddname indicated in the message specifies a nonprimary data set.

System action: Processing stops.

System programmer response: Correct the DD statements and rerun the job.

---

IRR67158I  DD ddname is not a backup data set. The following message shows the expected backup data set.

Explanation: The DD statement for INDD1 specifies a backup data set. Therefore, the utility expects all data sets to be backup data sets. However, the ddname indicated in the message specifies a nonbackup data set.

System action: Processing stops.

System programmer response: Correct the DD statements and rerun the job.

---

IRR67159I  The data set specified for INDD1 is primary or backup, but it is not the first entry in ICHRDSNT.

Explanation: The DD statement for INDD1 specifies a data set that is either primary or backup. Therefore, INDD1 must be the first data set listed in the data set name table (ICHRDSNT). The ddname indicated in the message specifies a data set that is either primary or backup and not the first entry in ICHRDSNT.

System action: Processing stops.

System programmer response: Correct the DD statements, and rerun the job.

---

IRR67160I  Internal error in the utility.

Explanation: An error occurred in the processing of the utility.

System action: Processing stops.

System programmer response: Report this message to your IBM support center. Include the following information: Interpreted JCL and SYSOUT.

---

IRR67161I  Failed write for DD ddname.

Explanation: An error occurred while writing to the indicated data set.

System action: Processing stops.

System programmer response: This can be caused by a problem with the ddname indicated in the message.

Problem Determination: This message is accompanied by messages issued by DFP. Follow the problem determination procedure for the DFP messages.

---

IRR67162I  Dataset is data-set-name on volume volume.

Explanation: This message identifies a RACF database described in an earlier message. If the device containing data-set-name has been dynamically reconfigured from the system, *VA replaces the volume information in the message.

System action: See “System Action” for the earlier message.
IRR67163I  INDD1 is a primary data set. All input data sets must be primary data sets.

Explanation: The DD statement for INDD1 specifies a primary data set. Therefore, the utility expects all data sets to be primary data sets.

System action: Processing continues normally.

IRR67164I  INDD1 is a backup data set. All input data sets must be backup data sets.

Explanation: The DD statement for INDD1 specifies a backup data set. Therefore, the utility expects all data sets to be backup data sets.

System action: Processing continues normally.

IRR67165I  The RACF data set name table (ICHRDSNT) indicates that there are nn RACF data sets, but only one was specified.

Explanation: The utility can process either your entire RACF database or a single data set of a multi-data set database. The utility has determined that you are processing a single data set from a multi-data set database.

System action: Utility processing continues.

System programmer response: You may ignore the count in IRR67150I if you are attempting to process a single data set from a multi-data set database.

IRR67166I  Processing continues using as input the data set specified as INDD1.

Explanation: The utility can process either your entire RACF database or a single data set of a multi-data set database. The utility has determined that you are processing a single data set from a multi-data set database.

Be sure to examine the output of the utility for any occurrences of the IRR67092I message with a return code of X'00000012' and reason code of X'00000000', which can occur when a user profile is contained in a separate database from its connect profiles. This can happen if your range table splits the database at a boundary between user profiles and connect profiles.

Note: This can only occur if your range table splits the database with a value that has two consecutive null values, such as 'XC10000C1'. If your range table has such a value, you must process all parts of your database in one execution of the utility.

IRR67167I  Multiple OUTDD statements were specified, but only one INDD was specified.

Explanation: The number of INDDx statements must be identical to the number of OUTDDx statements.

System programmer response: Execute the utility specifying the same number of INDDx and OUTDDx statements.

System action: Utility processing stops.

IRR67168I  Multiple INDD statements were specified, but only one OUTDD was specified.

Explanation: The number of INDDx statements must be identical to the number of OUTDDx statements.

System programmer response: Execute the utility specifying the same number of INDDx and OUTDDx statements.

System action: Utility processing stops.

IRR67169I  Database LOCKINPUT/UNLOCKINPUT parameters are not permitted while the system is in read-only mode.

Explanation: LOCKINPUT/UNLOCKINPUT attempts to update the extend bit in the ICB. However, no database updates can be made while the system is in read-only mode.

System action: Utility processing stops.

System programmer response: You can do one of the following tasks:
- Run IRRDBU00 with a parameter of LOCKINPUT/UNLOCKINPUT from another system that is not in read-only mode.
- Issue RVARY DATASHARE to change the mode of all systems to data sharing mode and rerun the job.
- Issue RVARY NODATASHARE to change the mode of all systems to non–data sharing mode and rerun the job.

IRR67180I  Unable to open data-set-name associated with DD dname.

Explanation: An error occurred while attempting to open the specified database.

System action: Processing stops.

System programmer response: To recover from the problem, ensure that the DD statement is correct.

Problem Determination: Check for other errors related to the disk pack on which the data set resides.
IRR67181I  Information retrieval for DD ddname failed with error code error-code.

Explanation: The utility issued a dynamic allocation request (SVC 99) for information about the ddname indicated in the message. However, the return code from dynamic allocation was unexpected.

System programmer response: See “Problem Determination.”

Problem Determination: Check the return code from the SVC 99 in [z/OS MVS Programming: Authorized Assembler Services Guide]

System action: Processing stops.

IRR67182I  data-set-name associated with DD ddname has been successfully opened.

Explanation: The specified data set is now open so that the utility can read from it or write to it.

System action: Processing continues normally.

IRR67183I  DD ddname not found.

Explanation: The specified DD was expected, but not found. If you are processing a single data set of a multi-data set database, you can ignore this message for INDD2.

System action: If the ddname is INDD2, processing continues. For any other ddname, processing stops.

System programmer response: Ensure that the number of INDDx statements is the same as indicated by message IRR67150I.

Problem Determination: Check the DD statements of the job to verify that the correct number of INDDs and OUTDDs are allocated.

IRR67240I  DD ddname could not be unlocked because of a write failure.

Explanation: An error occurred while attempting to unlock the specified input database.

System action: Utility processing stops.

System programmer response: To recover from the problem, consider doing the following tasks:

- Ensure that the DD statement is correct.
- If you are processing primary databases, switch to a backup RACF database (using the RVARY SWITCH command).

Note: For complete information about recovering from the problem, see the section on RACF database recovery in [z/OS Security Server RACF System Programmer’s Guide] Pay particular attention to the section on failures during I/O operations on the RACF database.

Problem Determination: Other messages might have been issued for this problem. An analysis of those messages might help you determine the cause of the problem. In particular, look for message ICH5101I, which reports a return code from the RACF manager.

IRR67241I  Unlock was successful. DD ddname is now unlocked.

Explanation: The RACF database indicated by the ddname can now be updated.

System action: Utility processing continues.

IRR67242I  DD ddname is already unlocked.

Explanation: You asked to unlock a database that is already unlocked.

System action: Utility processing continues.

IRR67243I  DD ddname could not be unlocked because of a read failure.

Explanation: An error occurred while attempting to read the specified input data set's ICB to determine its lock status.

System action: Utility processing stops.

System programmer response: To recover from the problem, consider doing the following tasks:

- Ensure that the DD statement is correct.
- If you are processing primary databases, switch to a backup RACF database (using the RVARY SWITCH command).

Note: For complete information about recovering from the problem, see the section on RACF database recovery in [z/OS Security Server RACF System Programmer’s Guide] Pay particular attention to the section on failures during I/O operations on the RACF database.

Problem Determination: Other messages might have been issued for this problem. An analysis of those messages might help you determine the cause of the problem. In particular, look for message ICH5101I, which reports a return code from the RACF manager.

IRR67244I  Unlock processing was attempted in read-only mode, which is not allowed. Data sets may still be locked.

Explanation: LOCKINPUT processing began in either non-data sharing mode or data sharing mode and may have locked data sets. At the start of the unlock portion of LOCKINPUT processing, it was found that the system is in read-only mode.

System action: Utility processing ends abnormally.
System programmer response: You can do one of the following tasks:

- Run IRRDBU00 with a parameter of UNLOCKINPUT from another system that is not in read-only mode.
- Issue RVARY DATASHARE to change the mode of all systems to data sharing mode and rerun the job.
- Issue RVARY NODATASHARE to change the mode of all systems to non-data sharing mode and rerun the job.

IRR67270I  error-message-text on ddname while attempting a request of a block at RBA rba

Explanation: The indicated error occurred while attempting a BDAM read (READ) or BDAM write (WRITE).

System action: The ddname of the file on which the error occurred is listed, along with the RBA (relative byte address) of the byte being accessed.

System programmer response: To recover from the problem, ensure that the DD statement is correct.

Problem Determination: Check for other errors related to the disk pack on which the database resides.

IRR67271I  A coupling facility related error occurred during database LOCKINPUT/UNLOCKINPUT processing for ddname.

Explanation: While writing the ICB to the coupling facility, the utility detected an error. The ddname of the file on which the error occurred is listed.

System action: Utility processing ends abnormally.

System programmer response: Check the SYSPRINT. Also, check the information specified in message IRRX016I, which is issued to the system console.

If the error occurred during the locking of the data sets, they have not been unloaded. If any data sets have been locked, you should either:

- Rerun the job from the original system if it is still in data sharing mode. You should specify the UNLOCKINPUT parameter first, followed by the LOCKINPUT parameter.
- Rerun the job from another system in the RACF sysplex data sharing group, if that system is in data sharing mode. You should specify the UNLOCKINPUT parameter.

If the error occurred during the unlocking of the data sets, you should either:

- Rerun the job from the original system if it is still in data sharing mode. You should specify the UNLOCKINPUT parameter.
- Rerun the job from another system in the RACF sysplex data sharing group, if that system is in data sharing mode. You should specify the UNLOCKINPUT parameter.
IRR67335I  I/O error occurred while trying to read the ICB for  
dsname DD ddname.
Explanation: The ICB (inventory control block) for the
specified RACF database cannot be read.
System action: Utility processing stops.
System programmer response: To recover from the
problem, ensure that the DD statement is correct.
Problem Determination: Check for other errors
related to the disk pack on which the database resides.

IRR67417I  RACF created a down level ACEE.
Database unload requires at least a level 2 ACEE.
Explanation: The accessor environment element
(ACEE) must be at least level 2.
System action: Utility processing stops.
System programmer response: Ensure that RACF
version 1.9.0 or later is properly installed on the
system.
Problem Determination: If this message recurs,
contact your IBM support center.

IRR67422I  Incorrect blocksize specified for INDD1.
The blocksize must be 4096.
Explanation: The data set that is specified as INDD1
must have a blocksize of 4096. The data set specified as
INDD1 had a blocksize of other than 4096.
System action: Utility processing stops.
System programmer response: Specify a valid data set
as INDD1.
Problem Determination: Check the INDD1 DD
statement.

IRR67423I  Open failed for OUTDD.
Explanation: An error occurred while attempting to
open the output data set.
System action: Utility processing stops.
Problem Determination: Ensure that OUTDD is
specified.

IRR67460I  *** Profile unloading not started ***
Explanation: Database unloading was not attempted
because of a prior failure in setting up the utility.
System action: Utility processing stops.
System programmer response: Ensure that the proper
initializations were made before executing the unload
utility. Rerun the utility after correcting errors identified
in previous messages.
Problem Determination: This message is displayed
after an error has been encountered. Use the messages
before this one to help determine what the specific
problem is.

IRR67494I  profile-count profile-type [class-name]  
profile(s) have been unloaded.
Explanation: This is an informational message
identifying the number and the type of the profiles that
the Database Unload Utility has just unloaded. The
class-name is only displayed for general resource
profiles.
System action: Processing continues.

IRR67495I *** Unloading not completed. ***
Explanation: The Database Unload Utility detected an error condition. Output is not complete.
System action: Processing halts.
Problem Determination: Examine the previous messages.

IRR67500I The Field Definition Table (FDT) and the ACTN area do not match. The unknown field is ccccccccc.
Explanation: An internal error has occurred.
Severity: Error
User response: Call the IBM support center.
System action: Utility processing stops.

IRR67520I Unable to establish recovery environment. Processing terminated.
Explanation: An ESTAE environment cannot be established.
System action: Utility processing stops.
User response: Ensure that RACF and the operating system are properly installed. If they are, report this message (and its message ID) to your IBM support center.

IRR67522I Open failed for ddname.
Explanation: An error occurred while attempting to open the specified ddname.
System action: Utility processing stops.
User response: Ensure that one of the following DD names is specified: OUTDD, XMLOUT, XMLFORM.

IRR67524I A pre-RACF 1.9 record was encountered in the input stream. The record is ignored.
Explanation: The input contains a record created by an unsupported version of RACF. Because this utility can process only SMF records that were created by RACF Version 1.9.0 or later, the record is ignored. Message IRR67581I identifies the failing record in more detail.
System action: Utility processing continues.

IRR67534I IRRADU00 UNSUCCESSFUL: CANNOT OPEN ADUPRINT.
Explanation: IRRADU00 cannot open the required sysprint file ADUPRINT. This message is issued by a write-to-operator (WTO) request.
System action: Utility processing stops.
User response: Allocate the file ADUPRINT before executing the utility.

IRR67540I The LRECL of the output data set allocated to ddname has been changed from original_lrecl to new_lrecl.
Explanation: The logical record length (LRECL) of the output data set was original_lrecl, which was smaller than that which is required by the utility. The utility has set the LRECL of the output data set to new_lrecl.
System action: Utility processing continues.

IRR67541I The BLKSIZE of the output data set allocated to ddname has been changed from original_block_size to new_block_size.
Explanation: The block size of the output data set was original_block_size, which was smaller than that which is required by the utility. The utility has set the BLKSIZE of the output data set to new_block_size. Note that the block size of the output data set must be at least 4 bytes larger than the logical record length.
System action: Utility processing continues.

IRR67550I abend_code abend during utility processing. Reason code rsncode.
Explanation: A system abend occurred during utility processing.
System action: Utility processing continues with the recovery procedure.
User response: For more information about the indicated abend, see an MVS system codes documentation.

IRR67551I The module in control at time of abend was module_name.
Explanation: The internal module that was in control at the time of the abend is listed here for debugging purposes.
System action: Utility processing continues with the recovery procedure.
User response: This message is accompanied by message number IRR67550I. If the problem recurs after following the problem determination for the above message number, then record all the information
provided by these two messages and contact your IBM support center.

IRR67552I  *** Utility ESTAE error routine in control. ***

Explanation: The recovery procedure for the utility is now running.

System action: Recovery processing begins.

IRR67580I Unexpected relocate section found in type record_type record for event code event_code/event_code_qualifier. The relocate number is relocate_number.

Explanation: This error message indicates that the SMF record being processed contained an unexpected relocate section. The type of the record is record_type. The unexpected relocate section is relocate_number. Event_code/event_code_qualifier are the event code and event code qualifier for the record.

Message IRR67581I identifies the failing record in more detail.

System action: Utility processing continues.

User response: Perform these steps:
1. Obtain a hexadecimal print of the failing record from the input supplied to the utility. You can use the MVS utilities IDCAMS or DITTO or their equivalent for this.
2. Compare the relocate sections that you find in the record with the relocate sections that are defined as valid for the specific event code. You can find a list of event codes, relocate sections, and the components that created the record, in z/OS MVS System Management Facilities (SMF) and z/OS Security Server RACF Macros and Interfaces.
3. Contact the IBM support center.

IRR67581I The failing record, relative_record, was created on date at time for user userid in group groupid on system smf_id.

Explanation: This message identifies the failing record for which message IRR67580I, IRR67524I, IRR67654I, or message IRR67655I was created.

System action: Utility processing continues.

User response: Use this information to locate the failing record so that you can find the failing profile. Relative_record might be useful when using print utilities such as IDCAMS and DITTO, which allow the specification of a relative record number. See z/OS DFSMS Access Method Services for Catalogs for more information about these utilities.

Note that the relative record number is the number of the record as it was passed to IRRADU00. This number may differ from the relative record number in the data set that was input to IFASMFDP if the IFASMFDP control statements suppressed the processing of some record type. See z/OS MVS System Management Facilities (SMF) for more information about the control statements for IFASMFDP.

IRR67582I The data associated with the relocate section is "relocate_data" and has a length of relocate_data_length.

Explanation: This message describes the data (relocate_data) associated with the unexpected relocate section that was identified in message IRR67580I. The length associated with the relocate section is shown as relocate_data_length. If the length of the data exceeds 16 bytes, only the first 16 bytes are shown in the message.

System action: Utility processing continues.

IRR67650I SMF data unload utility has successfully completed.

Explanation: IRRADU00 has successfully finished processing.

System action: Utility processing continues.

IRR67651I SMF data unload utility has not successfully completed.

Explanation: IRRADU00 found one or more errors during processing.

User response: Review the messages produced by both IRRADU00 and the system. Take the actions indicated in the messages.

IRR67652I The utility processed record_count SMF type record_type records.

Explanation: This informational message describes the number of records processed (record_count) for each type of record (record_type) that the utility processes.

System action: Utility processing continues.

IRR67653I The utility bypassed record_count SMF records not related to IRRADU00.

Explanation: This informational message tells you how many records (record_count) that were bypassed by the utility. The utility processes these SMF record types:
- type 30 ("Job initiation")
- type 80 ("RACF processing")
- type 81 ("RACF initialization")
- type 83 (subtype 1, "RACF auditing data sets") and (subtype 2 and above, "Security-related product events")

See z/OS MVS System Management Facilities (SMF) and z/OS Security Server RACF Macros and Interfaces for a complete description of these records.

System action: Utility processing continues.
IRR67654I The SMF record type 83 subtype subtype for product product with FMID fmid is unknown.

Explanation: This message describes an unexpected SMF type 83 record subtype.
System action: Utility processing continues.

IRR67655I The utility processed record_count SMF.

RACF remove ID utility (IRR RID00) messages

IRR68001I No IDs were found in the SYSIN data set. A search for all residual references is being performed.

Explanation: Since you did not specify one or more IDs for IRR RID00 to search for, a search is being made for all residual references. Possible causes of IRR RID00 not finding any IDs are: SYSIN was not allocated correctly, SYSIN was allocated to DUMMY, or SYSIN was not specified.
System action: Utility processing continues.
User response: If you intended to search for all residual references, no action is required. Otherwise, correct the SYSIN statements and submit the job again.

IRR68002I IRR RID00 found count records with inconsistent IDs.

Explanation: IRR RID00 found the indicated number of places in the database in which an ID value was used inconsistently. IRR RID00 verifies that in those places where only a user ID is valid, only a user ID is used. Similar verification is performed for group IDs. This message tells you how many times IRR RID00 found an ID value that was used improperly. Each occurrence of the improper ID is flagged with messages IRR68017I and IRR68018I.
System action: Utility processing continues.

IRR68003I DDNAME ddname did not open.

Explanation: The required DDNAME ddname cannot be opened.
System action: Utility processing stops with a decimal return code of 16.
User response: Correct the JCL and submit the job again.

IRR68004I IRR RID00 found count references.

Explanation: IRR RID00 detected the indicated number of references to the user IDs and group IDs you supplied.
System action: Utility processing continues.

IRR68005I IRR RID00 UNSUCCESSFUL: CANNOT OPEN SYSPRINT.

Explanation: IRR RID00 cannot open the required SYSPRINT file. This message is issued by a write-to-programmer (WTP) request.
System action: Utility processing stops, with decimal return code 20.
User response: Allocate the SYSPRINT file before running the utility. Correct the JCL and submit the job again.

IRR68006I The LRECL of the output data set allocated to OUTDD has been changed from original_lrecl to new_lrecl.

Explanation: The logical record length (LRECL) of the output data set was original_lrecl, which was smaller than required by the utility. The utility has set the LRECL of the output data set to new_lrecl.
System action: Utility processing continues.

IRR68007I The BLKSIZE of the output data set allocated to OUTDD has been changed from original_block_size to new_block_size.

Explanation: The block size of the output data set was original_block_size, which was smaller than required by the utility. The utility has set the BLKSIZE of the output data set to new_block_size. Note that the block size of the output data set must be at least 4 bytes larger than the logical record length.
System action: Utility processing continues.

IRR68008I *** Utility ESTAE error routine in control. ***

Explanation: The recovery procedure for the utility is now processing. This message is accompanied by message number IRR68009I and IRR68010I.
System action: Recovery processing begins and utility processing stops with a decimal return code of 16.
User response: Follow the user responses specified in messages IRR68009I and IRR68010I.
IRR68009I  abend_code  Abend occurred during utility processing. The reason code is reason_code.

Explanation: An abend occurred during utility processing. This message is accompanied by message numbers IRR68008I and IRR68010I. abend_code is a six-hexadecimal-character string in which the first three hexadecimal characters are the system abend code and the last three hexadecimal characters are the user abend code. reason_code is also a hexadecimal character string.

System action: Utility processing continues with the recovery procedure.

User response: For more information about the indicated abend, see z/OS MVS System Codes and correct the problem.

IRR68010I  The module in control at the time of the abend was module_name - text.

Explanation: The internal module that was in control at the time of the abend is listed here for debugging purposes. The text displayed describes the last function attempted by the indicated module. This message is accompanied by message numbers IRR68008I and IRR68009I.

System action: Utility processing continues with recovery procedure.

User response: If the problem recurs after following the user response for the indicated message numbers, record all information provided by all the messages and contact your IBM support center.

IRR68011I  The utility has successfully completed.

Explanation: IRRRID00 has successfully finished processing. The decimal return code is zero.

IRR68012I  The utility has not successfully completed.

Explanation: IRRRID00 found one or more errors during processing.

User response: Review the messages produced by both IRR RID00 and the system. Take the actions appropriate to correct the problem.

IRR68013I  The failing record number record_number in INDD was not produced by IRRDBU00.

Explanation: IRRRID00 requires that valid IRRDBU00 output be used as input to INDD. IRRRID00 has determined that the record record_number was not generated by IRRDBU00.

System action: Utility processing stops with a decimal return code of 16.

User response: Be sure that INDD was allocated to a data set created by IRRDBU00 and that the data set's DCB characteristics are valid IRRDBU00 data set characteristics, specifically, that the record format is variable blocked (VB).

IRR68014I  function_name has completed with a return code of return_code.

Explanation: A function has returned a non-zero return code. function_name is the identifier of the function. If function_name is "SORT", then a call to the SORT product has returned a non-zero hexadecimal return code. If function_name is "ESTAE ESTABLISHMENT", then the establishment of the ESTAE recovery routine failed. return_code is the hexadecimal return code.

System action: Utility processing stops with a decimal return code of 16.

User response: Review the messages produced by the sort utility and take the actions indicated by those messages.

IRR68015I  Record number record_number in INDD was not produced by IRRDBU00.

Explanation: IRRRID00 requires that valid IRRDBU00 output be used as input to INDD. IRRRID00 has determined that the record record_number was not generated by IRRDBU00.

System action: Utility processing stops with a decimal return code of 16.

User response: Be sure that INDD was allocated to a data set created by IRRDBU00 and that the data set's DCB characteristics are valid IRRDBU00 data set characteristics, specifically, that the record format is variable blocked (VB).

IRR68016I  IRRRID00 was forced to truncate count records.

Explanation: The commands created by IRRRID00 are limited to 255 character lines. count is the number of commands that were created in which IRRRID00 cannot fit the profile name or member data into a 255 character line. A question mark (?) in the left column shows the command lines that have been truncated.

System action: The utility truncates the line on the right, sets the utility decimal return code to 4, and continues processing.

User response: Review the truncated command that IRRRID00 created and process it manually if required.

IRR68017I  The ID id in the class profile profile_name is not correct.

Explanation: IRRRID00 has found a profile containing an ID value that was not of the correct class. For example, the NOT IFY field must contain a user ID. If it contained a group ID, this message would be issued. ID is the ID value that is in error. class is the class of this profile. profile_name is the name of the profile, truncated to 20 characters.
**System action:** The utility places commands to correct the error (for example, deleting all references of the 'ID') into the OUTDD data set. Message IRR68018I follows this message. The utility continues processing.

**User response:** Review and verify all references of the ID should be deleted, and if necessary, edit the commands created by IRRRID00.

**Explanation:** This message identifies the profile that contains an incorrect ID value. record_number is the relative number of the input record that contained the ID value. class is the class that the ID value should be. Message IRR68017I precedes this message.

**System action:** The utility continues processing.

**User response:** Review and, if necessary, edit the commands created by IRRRID00.

**IRR68019I** IRRRID00 has searched s_count records and processed l_count records. (hh:mm:ss)

**Explanation:** Periodically, IRRRID00 indicates the number of IRRDBU00 records that it has processed. hh:mm:ss is the time that the message was issued. s_count is the number of records that have been searched for residual IDs. l_count is the number of records that have been processed, from which commands are generated.

This message is issued only if you have not supplied any user IDs or group IDs to search for.

You can look at the messages produced by the SORT program to see the total number of records that are being processed.

**System action:** The utility continues processing.

**User response:** None. This message is for informational purposes only.

**IRR71001E** No arguments were specified for the function.

**Explanation:** A variable name was not specified for the RACVAR function. A variable name is required in the form RACVAR(variable-name).

**System action:** EXEC processing stops.

**User response:** Correct the RACVAR function and specify a valid variable name in the form RACVAR(variable-name).

**IRR71002E** This system variable xxx is not supported for RACVAR processing.

**Explanation:** The variable name specified for the RACVAR function is not valid.

**System action:** EXEC processing stops.

**User response:** Correct the RACVAR function and specify one variable name in the form RACVAR(variable-name).
System action: EXEC processing stops.

Explanation: No ACEE was available from which the information can be extracted.

User response: Log off and log on again. Reenter the request that caused this message. If this message is issued again, report the message (and the request you were making) to your system programmer.

---

**RACF subsystem messages**

**IRRA001I** UNABLE TO OBTAIN STORAGE FOR subsystem SUBSYSTEM ON INITIALIZATION.

Explanation: The subsystem has not been successfully initialized because of the failure of GETMAIN to obtain storage for the main subsystem control block.

System action: The initialization for the subsystem stops.

Operator response: Report the exact text of this message to your system programmer.

System programmer response: Make sure that sufficient storage is available in the common storage area (CSA) for this control block. For information about CSA storage estimates, see [z/OS Security Server RACF System Programmer’s Guide](https://www.ibm.com).}

Destination: Descriptor code is 6. Routing code is 2.

**IRRA002I** subsystem SUBSYSTEM HAS NOT BEEN INITIALIZED.

Explanation: The indicated subsystem has not been successfully initialized. One or more previous messages have been issued providing specific information.

System action: The initialization for the subsystem stops.

Operator response: Report this message to your system programmer.

System programmer response: See the previous messages for more specific information.

Destination: Descriptor code is 6. Routing code is 2.

**IRRA003I** subsystem SUBSYSTEM INITIALIZATION TERMINATED IN ABEND HANDLING.

Explanation: The initialization task for the indicated subsystem has detected an abend while attempting to process a previous abend.

System action: The task stops.

Operator response: Report this message to your system programmer.

System programmer response: Determine the cause for the abend from previous error messages.

Destination: Descriptor code is 4. Routing code is 2.

**IRRA004I** UNABLE TO LOCATE MODULE module IN PROGRAM PROPERTIES TABLE.

Explanation: Initialization for the RACF subsystem was not able to find the indicated module defined in the program properties table.

System action: The address space discontinues initialization.

Operator response: See the System Programmer Response or contact your system programmer.

System programmer response: Make sure that the correct PPT entry is defined in parmlib member SCHEDxx for the RACF subsystem mainline module.

**IRRA007I** The command prefix prefix could not be registered for subsystem subsystem. Return code X’recode’ and reason code X’rscode’ specify the MVS CPF error.

Explanation: The attempt to register command prefix prefix for subsystem subsystem failed with MVS command prefix facility (CPF) return code recode and reason code rscode.

System action: The RACF subsystem is not available.

System programmer response: See the MVS documentation on the CPF to determine the problem. Use the MVS DISPLAY OPDATA command, if necessary, to see if the command prefix is already registered.

The RACF subsystem is started out of proclib, the procname, which is the subsystem name, is identified within the active IEFSSNxx member from parmlib by INITRTN(IRRSI00) and the command prefix is also set there by the INITPARM parameter. If you restart the RACF subsystem after a failed attempt to register the command prefix, the subsystem uses the default command prefix, the subsystem name, (for example: START xxxx, SUB=MSTR).

**IRRA008I** The system is in XCF-local mode. Scope of the command prefix prefix for subsystem subsystem has defaulted to SYSTEM.

Explanation: The requested sysplex scope defaulted to SYSTEM scope for the indicated subsystem because the system is running in XCF-local mode.

System action: Initialization continues.
Operator response: Notify the system programmer.

System programmer response: Correct the scope in the IEFSSNxx parmlib member parameter. If needed, IPL the system for the change to take effect.

Destination: Descriptor code is 4. Routing code is 2.

IRRA009I Error encountered while processing the IEFSSNxx for the subsystem subsystem. CPF system-wide default will be used.

Explanation: An incorrect value was encountered while processing the IEFSSNxx parmlib member for the subsystem subsystem parameter. CPF system-wide default is used.

System action: Initialization continues. Subsequent subsystem commands have only a system-wide scope.

System programmer response: Correct the scope in the IEFSSNxx parmlib member parameter. If needed, IPL the system for the change to take effect.

Destination: Descriptor code is 4. Routing code is 2.

IRRA010I Error encountered while processing the IEFSSNxx for the subsystem subsystem. Prefix will be truncated to eight characters.

Explanation: An incorrect value was encountered while processing the IEFSSNxx parmlib member for the subsystem subsystem parameter. The prefix is truncated.

System action: Initialization continues.

System programmer response: Correct the length of the IEFSSNxx parmlib member parameter. If needed, IPL the system for the change to take effect.

Destination: Descriptor code is 4. Routing code is 2.

IRRA011I OUTPUT FROM command-name:

Explanation: A RACF command was issued from the operator console. After this message is issued, the output from command command-name is displayed at the operator console.

Destination: Descriptor codes are 5 and 6. Routing code is 2.

IRRA080I subsystem SUBSYSTEM INITIALIZATION ENCORUNCERED AN ERROR. ABEND CODE IS cde-rc.

Explanation: The initialization task for the indicated subsystem has encountered an abnormal condition.

System action: The task attempts to restart.

Operator response: Contact your system programmer.

System programmer response: The system abend dump contains more detailed information regarding the problem encountered by the indicated subsystem initialization task.

IRR8000I subsystem SUBSYSTEM NOT DEFINED TO SYSTEM, TERMINATING.

Explanation: The subsystem name could not be located in the SSCT control blocks. The subsystem being searched for is indicated in the message.

System action: The subsystem stops.

Operator response: Report the exact text of this message to your system programmer.

System programmer response: Add the subsystem name to the appropriate MVS subsystem name table (see IEFSSNxx PARMLIB member).

Destination: Descriptor code is 6. Routing code is 2.

IRR8001I subsystem SUBSYSTEM ver.rel.mod IS ACTIVE.

Explanation: Subsystem subsystem is active. The version is ver, the release is rel, and the modification is mod.

System action: None.

Operator response: None.

Destination: Descriptor code is 6. Routing code is 2.

IRR8002I INITIALIZATION COMPLETE FOR subsystem SUBSYSTEM

Explanation: All of the initialization for the indicated subsystem environment has been completed.

System action: The subsystem is ready to accept operator commands.

Operator response: None.

Problem Determination: None.

Destination: Descriptor code is 6. Routing code is 2.

IRR8003I subsystem SUBSYSTEM NOT RUNNING AS A STARTED TASK.

Explanation: The indicated subsystem was not started as a started task.

System action: The subsystem stops.

Operator response: Report the exact text of this message to your system programmer.

System programmer response: Restart the indicated subsystem as a started task. (This message could reflect an error in the ICHRIN03 started task table).

Destination: Descriptor code is 6. Routing code is 2.
IRRB004I  RACF SUBSYSTEM ALREADY ACTIVE.
Explanation: An attempt was made to start another RACF subsystem while the current subsystem is still active. RACF does not allow more than one RACF subsystem to be active.
System action: The command is terminated.
System programmer response: If no RACF subsystem is active, verify that the ENQ resource (major name SYSZRACF and minor name RACF) was not propagated from some other system.
Destination: Descriptor code is 6. Routing code is 2.

IRRB005I  subsystem SUBSYSTEM TERMINATION IS COMPLETE.
Explanation: The indicated subsystem stops.
System action: None.
Operator response: Check accompanying message and take appropriate action.
Destination: Descriptor code is 6. Routing code is 2.

IRRB006I  subsystem SUBSYSTEM MAIN TASK ABENDED IN ABEND HANDLING.
Explanation: While attempting to handle an abend the indicated subsystem task encountered another abend in abend-handling code.
System action: The subsystem stops.
Operator response: Report the exact text of this message to your system programmer.
System programmer response: Examine console log and system abend dumps for more detailed information. Determine the cause of the first abend and restart.
Destination: Descriptor code is 6. Routing code is 2.

IRRB007I  RESTART LIMIT nn EXCEEDED FOR TASK taskname IN subsystem subsystem.
Explanation: The task indicated by taskname has exceeded the limit nn for automatic restarts by the main task in the indicated subsystem.
System action: Task taskname is not restarted.
Operator response: Report the exact text of this message to your system programmer.
System programmer response: Examine the console log for abend messages about the particular problem.
Destination: Descriptor code is 6. Routing code is 2.

IRRB008I  subsystem IS NOT OPERATING IN AN AUTHORIZED MODE.
Explanation: The job step failed APF authorization.
System action: The indicated subsystem stops.
Operator response: Report the exact text of this message to your system programmer.
System programmer response: Ensure that RACF subsystem modules are linked into an authorized library with AC(1).
Destination: Descriptor code is 6. Routing code is 2.

IRRB009I  subsystem SUBSYSTEM INTERFACE MODULE xxxxxxxx COULD NOT BE FOUND.
Explanation: The named subsystem could not locate the indicated subsystem interface module.
System action: The subsystem stops.
Operator response: Report the exact text of this message to your system programmer.
System programmer response: Ensure that the module indicated in the message is in LNKLSTxx library.
Destination: Descriptor code is 6. Routing code is 2.

IRRB010I  subsystem SUBSYSTEM INITIALIZATION FAILED TO BUILD THE SUBSYSTEM VECTOR TABLE.
Explanation: The subsystem interface module found that the number of address vectors contained in the address vector table module exceeded the available number of entries in the SSVT table.
System action: The indicated subsystem stops.
Operator response: Report this message to your system programmer.
System programmer response: Make sure that the address vector table module is at the proper level with respect to the size of the SSVT table.
Destination: Descriptor code is 6. Routing code is 2.

IRRB011I  UNABLE TO OBTAIN STORAGE FOR subsystem subsystem.
Explanation: Initialization for subsystem subsystem could not obtain storage for subsystem control blocks in common storage.
System action: The subsystem is not initialized.
Operator response: Report the text of this message to your system programmer.
System programmer response: Determine the cause of
the storage shortage, fix the problem, and restart the address space.

Note: Storage for subsystem control blocks is in CSA (not ECSA).

Destination: Descriptor codes is 6. Routing code is 2.

IRR012I subsystem INITIALIZATION HAS RETURNED AN UNKNOWN RETURN CODE rc.

Explanation: Initialization for the indicated subsystem returned an unexpected return code.

System action: The subsystem stops.

Operator response: Report this message to your system programmer.

System programmer response: Report the exact text of this message to your IBM support along with a list of recently applied RACF maintenance.

Destination: Descriptor code is 6. Routing code is 2.

IRR013I RACF IS NOT ACTIVE. subsystem SUBSYSTEM TERMINATED.

Explanation: The subsystem does not operate unless RACF is active.

System action: The subsystem stops.

Operator response: Report the exact text of this message to your system programmer.

System programmer response: Determine cause of RACF failure, reactive RACF, and restart the subsystem.

Destination: Descriptor code is 6. Routing code is 2.

IRR014I subsystem SUBSYSTEM IS NOT OPERATING UNDER A RACF-DEFINED USERID.

Explanation: The subsystem does not have a valid user ID associated with it. This could occur for the following reasons:

• No user ID has been associated with the subsystem in either the STARTED class or the started procedures table (ICHRIN03).
• The user ID associated with the subsystem has not been defined to RACF.
• A valid user ID was specified but is not connected to the specified group.

System action: The subsystem stops.

Operator response: Report the exact text of this message to your system programmer.

System programmer response: If your installation is using the started procedures table to associate user IDs with started procedures, enter a valid RACF user ID in the started procedures table entry for the subsystem named in the message and reIPL. For more information about this table, see z/OS Security Server RACF System Programmer’s Guide. Verify with the security administrator that the user ID is defined to RACF. If your installation is using the STARTED class, report this message to the security administrator.

RACF Security Administrator Response: Define the user ID to be associated with the subsystem named in the message, if one is not already defined. If your installation is using the STARTED class to associate user IDs with started procedures, define a profile in the STARTED class that associates the user ID with the subsystem named in the message, if one is not already defined. For more information about the STARTED class, see z/OS Security Server RACF Security Administrator’s Guide.

Destination: Descriptor code is 6. Routing code is 2.

IRR015I taskname TASK IN subsystem SUBSYSTEM HAS TERMINATED ABNORMALLY.

Explanation: During the shutdown process, the subtask taskname in the subsystem subsystem would not voluntarily shut down. The main task has waited a sufficient interval for the subtask to end, without success. The subtask is forcefully ended.

System action: Subtask taskname ends abnormally. The subsystem continues the shutdown process.

Operator response: Report the exact text of this message to your system programmer.

System programmer response: Examine any system dumps obtained.

Destination: Descriptor code is 6. Routing code is 2.

IRR016I subsystem SUBSYSTEM NOT SUPPORTED IN THIS ENVIRONMENT

Explanation: The subsystem subsystem is only supported on MVS systems at or above the 3.1.3 level. The subsystem has detected that the current operating environment does not meet this requirement. You can also get this message when RACF initialization fails to complete successfully.

System action: Subsystem subsystem stops.

User response: Report the exact text of this message to your system programmer.

System programmer response: Do not attempt to exercise this function on an MVS system below the indicated level.

Destination: Descriptor code is 6. Routing code is 2.
IRRB017I • IRRB023I

IRRB017I  taskname TASK HAS ABENDED WITH A CODE OF cde-rc IN subsystem SUBSYSTEM.

Explanation: The main task has detected an MVS system completion code in subtask taskname as indicated by completion code cde, reason code rc in subsystem subsystem.

System action: The current command is ignored. The subsystem attempts to restart the subtask.

Operator response: None.

System programmer response: Determine the cause of the subtask abend.

Destination: Descriptor code is 6. Routing code is 2.

IRRB019I  MESSAGE message-number COULD NOT BE ISSUED DUE TO A FAILURE DURING MESSAGE PROCESSING.

Explanation: An error occurred while attempting to issue message message-number. The message is undefined or an I/O error occurred.

System action: Message processing for the requested message ends.

User response: Contact the system programmer. If the message exists in z/OS Security Server RACF Messages and Codes the most likely cause of this message is that an incomplete RACF service update was applied.

System programmer response: Verify service application for accuracy. If there is no problem with service application and this message persists, this indicates an I/O problem while issuing the message and requires further investigation.

Destination: Descriptor code is 6. Routing code is 2.

IRRB020I  task TASK HAS BEEN RESTARTED.

Explanation: The subsystem has restarted the task for which a prior RESTART command was issued.

Operator response: None.

IRRB021I  UNABLE TO LOAD SERVICE ROUTINE (routine). subsystem SUBSYSTEM TERMINATED.

Explanation: Service routine routine is needed for correct execution of the indicated subsystem but could not be loaded during initialization.

System action: The indicated subsystem stops.

Operator response: Notify the system programmer of the error.

System programmer response: Ensure that service routine routine resides in the LNKLST concatenation.

Destination: Descriptor code is 6. Routing code is 2.

IRRB022I  SUB=MSTR WAS NOT SPECIFIED ON THE START subsystem-name COMMAND. COMMAND IS IGNORED.

Explanation: A START command without the SUB=MSTR parameter was issued to start subsystem-name subsystem. subsystem-name is a RACF subsystem that can only be started under the master subsystem.

System action: The command is ignored. The specified RACF subsystem is not started.

Operator response: To start a RACF subsystem, issue the START command with the SUB=MSTR parameter.

Destination: Descriptor code is 6. Routing code is 2.

IRRB023I  SYSTEM SERVICE service FAILED WITH RETURN CODE return-code, REASON CODE reason-code.

Explanation: RACF invoked a UNIX service to dub the RACF subsystem address space as a UNIX process, but the service failed with the return and reason codes specified. RACF only invokes UNIX services during subsystem initialization if a RACF function that requires UNIX (for example, password enveloping) has been enabled. The most likely cause of this failure is that the subsystem address space identity does not have an OMVS segment. If so, you might see an ICH408I message in addition to IRRB023I.

Note: If the RACF subsystem address space has the PRIVILEGED attribute, the ICH408I message will not be displayed because audit records are not created for PRIVILEGED tasks

System action: The RACF subsystem continues to initialize. Functions that require z/OS UNIX system services are not available.

RACF Security Administrator Response: If the subsystem address space identity is not defined as a UNIX user, define an OMVS segment for its USER profile and for its default group profile. See z/OS Security Server RACF Security Administrator’s Guide for details on defining UNIX users. The RACF subsystem user ID does not require, and should not be assigned, a UID value of 0. Unless message IRRC040I was also issued, the RACF subsystem address space must be stopped and restarted after the OMVS information has been defined for the UNIX functions to become available. To avoid interruptions in services provided by the address space, it should be restarted during a period of low activity. See z/OS Security Server RACF System Programmer’s Guide for information about the RACF subsystem.

If the RACF subsystem address space identity is defined as a UNIX user, consult z/OS UNIX System Services Programming: Assembler Callable Services.
Reference for the meaning of the return and reason codes.

Destination: Descriptor code is 6. Routing code is 2.

**IRRB031I** TSO STACK HAS RETURNED A RETURN CODE OF **xx** IN **subsystem** SUBSYSTEM.

Explanation: The STACK macro returned a nonzero return code (xx) when an attempt was made to direct the input and output of a TSO command to specified files.

System action: The subsystem stops.

Operator response: Report the exact text of this message to your system programmer.

System programmer response: Using the xx value, determine the cause of the condition and correct it. For an explanation of the return code, see z/OS TSO/E Programming Services.

Destination: Descriptor code is 6. Routing code is 2.

**IRRB032I** **subsystem** SUBSYSTEM UNABLE TO OBTAIN STORAGE FOR **xxxx** CONTROL BLOCK.

Explanation: The storage requested by the GETMAIN for the xxxx control block was not available. The possible values for xxxx are PSCB, UPT, ECT, and LWA.

System action: Subsystem **subsystem** stops.

Operator response: Report the exact text of this message to your system programmer.

System programmer response: Ensure that a sufficient region size is specified on the subsystem JCL.

Problem Determination: See message IRRB038I for additional problem determination information.

Destination: Descriptor code is 6. Routing code is 2.

**IRRB033I** **subsystem** SUBSYSTEM UNABLE TO ALLOCATE FILE **subsystem** FOR TSO STACK USAGE.

Explanation: The dynamic allocation request for the input or output file to be used by the TSO STACK macro has failed. See message IRRB034I for more dynamic-allocation error information.

System action: The subsystem stops.

Operator response: Report the exact text of this message to your system programmer.

System programmer response: Ensure that the subsystem JCL permits dynamic allocation.

Destination: Descriptor code is 6. Routing code is 2.

**IRRB034I** DYNAMIC ALLOCATION INFORMATION: S99INFO IS **xxx**, S99ERROR IS **yyyy**.

Explanation: Dynamic allocation failed for either an input or an output file for use with the TSO STACK macro. This message follows the IRRB033I message.

System action: The subsystem stops.

Operator response: Report the exact text of this message to your system programmer.

System programmer response: Restart the subsystem after taking the action indicated for the dynamic-allocation error condition.

Destination: Descriptor code is 6. Routing code is 2.

**IRRB036I** OPERATOR COMMAND PREFIX (**subsystem-name**) MAY NOT BE AS SPECIFIED IN IEFSSNxx FOR **subsystem-name** SUBSYSTEM.

Explanation: The operator restarted the subsystem after one of the following conditions occurred:

- The initialization module failed to initialize the subsystem. Message IRRA001I is also issued.
- An operator was told to restart the subsystem manually with PARM=INITIAL.
- CPF registration was requested but failed. Message IRRA007I is also issued.

The subsystem name is used as the command prefix.

System action: RACF does not attempt to register the default command prefix (the subsystem name) with CPF as a result of this message. Subsystem initialization continues.

Operator response: Report the exact text of this message (IRRB036I) and message IRRB031I or IRRB037I, if either was issued, to your system programmer.

System programmer response: If message IRRA001I was issued, see the message explanation for that message.

If message IRRA007I was issued, see the return and reason codes given in that message for additional information in determining the problem.

Fix the problem before the next IPL. Use the default command prefix (the subsystem name) for this IPL.

Destination: Descriptor code is 6. Routing code is 2.

**IRRB037E** RESTART LIMIT OF **nn** EXCEEDED, **subsystem** SUBSYSTEM TERMINATED.

Explanation: The indicated subsystem mainline task has exceeded the limit for automatic restarts.

System action: The subsystem is not restarted.
IRRB038I   STORAGE REQUESTED IS yyyy;
            SUBPOOL IS zzz.
Explanation: This message is issued after IRRB032I, and indicates the storage and subpool requested by the GETMAIN.
System action: See message IRRB032I.
Operator response: See message IRRB032I.
System programmer response: See message IRRB032I.
Destination: Descriptor code is 6. Routing code is 2.

IRRB039E   ABEND ENCOUNTERED BEFORE subsystem SUBSYSTEM INITIALIZED.
Explanation: The indicated subsystem encountered an initialization failure and further processing for the subsystem stops.
System action: The subsystem stops.
Operator response: Report the exact text of this message to your system programmer.
System programmer response: See the console log or dumps, if any, to determine the problem.
Destination: Descriptor code is 6. Routing code is 2.

IRRB040I   RESTART BEING ATTEMPTED FOR ttttttt TASK.
Explanation: The task indicated by ttttttt has encountered an abend and is attempting to restart.
System action: The subsystem attempts to restart by detaching and reattaching the ttttttt task.
Operator response: Report the exact text of the message to your system programmer.
System programmer response: Examine the console log for previously issued RACF messages or dumps and determine the cause of the problem.
Destination: Descriptor code is 6. Routing code is 2.

IRRB041I   ttttttt TASK HAS ENDED WITH A CODE OF return-code IN subsystem SUBSYSTEM.
Explanation: The task indicated by ttttttt detached with an incomplete return code as indicated in return-code, which is displayed in hexadecimal format. The task may have ended because of an abend or the unexpected failure of a system service.
System action: RACF restarts the task and the RACF subsystem continues normal operation. Tasks automatically restart up to five times between address space initializations or between uses of the RESTART command for a particular task.
Operator response: Report the exact text of this message to your system programmer.
System programmer response: Examine the console log and any relevant system dumps to determine cause of abends. Attempt manual restart of the system by using PARM=INITIAL option.
Destination: Descriptor code is 11. Routing code is (1,9).

IRRB042I   TSO ENVIRONMENT SERVICE REASON CODE IS reason-code.
Explanation: IKJTSOEV returned the code reason-code following its invocation during subsystem initialization.
System action: The subsystem attempts to initialize.
System programmer response: See the appropriate TSO documentation for problem determination.
Destination: Descriptor code is 6. Routing code is 2.

IRRB043I   TSO ENVIRONMENT SERVICE DETAIL CODE IS code.
Explanation: IKJTSOEV returned the code code following its invocation during subsystem initialization.
System action: The subsystem attempts to initialize.
System programmer response: See the appropriate TSO documentation for problem determination.
Destination: Descriptor code is 6. Routing code is 2.

IRRB048I   subsystem-name SUBSYSTEM USING PREVIOUS JCL PARM SPECIFICATION OF: yy.
Explanation: The subsystem-name subsystem is initializing by using the value yy saved from a prior initialization. The RACF parameter library data set is as specified in the current JCL for the indicated subsystem.
System action: The subsystem-name subsystem attempts to initialize.
Operator response: None.
Destination: Descriptor code is 6. Routing code is 2.

IRRB049I  subsystem-name SUBSYSTEM IS NOT ABLE TO ESTABLISH TSO ENVIRONMENT, STATUS FOLLOWS:

Explanation: The TSO service IKJTSOEV failed. It was invoked by the indicated subsystem and is necessary for proper execution of that subsystem.

System action: The indicated subsystem ends.

Operator response: Report the text of this and related messages to the system programmer.

System programmer response: See related messages IRRB042I, IRRB043I, IRRB050I for a determination of the problem.

Destination: Descriptor code is 6. Routing code is 2.

IRRB050I  TSO ENVIRONMENT SERVICE RETURN CODE IS return-code.

Explanation: IKJTSOEV returned the code return-code following its invocation during subsystem initialization.

Operator response: Report the text of this and related messages to the system programmer.

System programmer response: See related message IRRB042I and appropriate TSO documentation for problem determination.

Destination: Descriptor code is 6. Routing code is 2.

IRRB064I  subsystem-name JCL PARM SPECIFICATION IS: yyyyyyyyyyyyyy.

Explanation: The subsystem-name is initializing by using the member yyyyyyyyyyyyy specified. If yyyyyyyyyyyyy specifies a valid parameter library member, the RACF parameter library data set (as specified in the current JCL of subsystem-name) is searched for the appropriate member whose configuration statements are to be processed.

System action: The subsystem-name subsystem attempts to initialize.

Operator response: None.
Destination: Descriptor code is 6. Routing code is 2.

IRRB065I  subsystem-name PARAMETER LIBRARY MEMBER SUFFIX STRING CONTAINS INCORRECT CHARACTER(y). SUFFIX IS IGNORED.

Explanation: A correct member suffix can contain only alphanumeric characters, and y is not alphanumeric.

System action: The indicated subsystem attempts to initialize without processing RACF parameter library configuration statements.

Operator response: The configuration statements that were to be processed by reference to a RACF parameter library member can be processed after subsystem initialization by using the SET INCLUDE command.

Destination: Descriptor code is 6. Routing code is 2.

IRRB066I  subsystem-name PARAMETER LIBRARY MEMBER SUFFIX STRING IS NULL. 00 IS ASSUMED.

Explanation: In the absence of a named suffix, 00 is used to form the name of the RACF parameter library member whose configuration statements are to be processed (IRROPT00).

System action: The indicated subsystem attempts to find the IRROPT00 member of the RACF parameter library and process its configuration statements.

Operator response: None.
Destination: Descriptor code is 6. Routing code is 2.

IRRB067I  subsystem-name PARAMETER LIBRARY MEMBER SUFFIX STRING IS LONGER THAN 2 CHARACTERS. SUFFIX IS IGNORED.

Explanation: The given suffix has a length that exceeds the allowed maximum.

System action: The indicated subsystem attempts to initialize without processing RACF parameter library configuration statements.

Operator response: The configuration statements that were to be processed by reference to a RACF parameter library member can be processed after subsystem initialization by using the SET INCLUDE command.

Destination: Descriptor code is 6. Routing code is 2.

IRRB068I  subsystem-name SUBSYSTEM WAS UNABLE TO BUILD ITS SCREEN TABLE. INITIALIZATION CONTINUES.

Explanation: An error during initialization of the subsystem-name subsystem prevents the successful delivery of output from directed RACF commands by way of TSO XMIT. The delivery of such output to user data sets is unaffected.

System action: Subsystem initialization continues.

Operator response: Report the text of this message to the system programmer.

System programmer response: Report the occurrence of the error to the IBM support center.

Destination: Descriptor code is 6. Routing code is 2.
IRRB069I subsystem-name SUBSYSTEM STARTING SHUTDOWN PROCESSING.

Explanation: The indicated subsystem has started shutdown processing in response to an operator STOP command.

System action: The indicated subsystem is in the process of ending all subsystem-related functions and stops.

Operator response: None.

Destination: Descriptor code is 6. Routing code is 2.

IRRB070I subsystem-name SUBSYSTEM UNABLE TO PERFORM RESTART.

Explanation: The indicated subsystem was not able to process the RESTART command at this time.

System action: RACF continues processing.

Operator response: Try the command again at a later time. If this message continues, issue the RESTART CONNECTION command. If the RESTART CONNECTION command also fails, you must stop the affected RACF subsystem address space by issuing the STOP subsystem-name command and then issue the MVS START command to start the started procedure for the RACF address space.

Destination: Descriptor code is 6. Routing code is 2.

IRRB071I node-name UNDEFINED. COMMAND NOT PROCESSED.

Explanation: The indicated node name is not defined to RRSF.

System action: RACF continues processing.

Operator response: Reenter the command and make sure that you type the correct node name.

Destination: Descriptor code is 6. Routing code is 2.

IRRB072I EXTRANEOUS CHARACTERS WERE FOUND AFTER STOP COMMAND FOR subsystem-name SUBSYSTEM. COMMAND NOT PROCESSED.

Explanation: Extraneous characters were found in the STOP command issued for subsystem subsystem-name.

System action: RACF continues processing.

Operator response: If you want to bring down the RACF subsystem address space, reenter the RACF STOP command without any trailing text.

Destination: Descriptor code is 6.

IRRB073I EXTRANEOUS TEXT DETECTED IN RESTART COMMAND. COMMAND function PROCESSED. EXTRANEOUS CHARACTERS WERE IGNORED.

Explanation: Extraneous characters were found after function function on the RESTART command. RESTART is valid only for one function at a time. All information specified after the first function is ignored.

System action: RACF ignores the extraneous characters and continues processing.

Operator response: None.

Destination: Descriptor code is 6.

IRRB074I INCORRECT KEYWORD ENCOUNTERED FOR RESTART.

Explanation: A RESTART command was issued with an incorrect keyword specified.

System action: The command is not processed but RACF continues processing.

Operator response: Reissue the RESTART command by using valid keywords.

Destination: Descriptor code is 6.

IRRB075I NOT AUTHORIZED TO ISSUE THE command COMMAND.

Explanation: The user attempting to issue the indicated command is not authorized to the correct profile in the OPERCMDS resource class.

System action: The indicated command ends without further processing.

Operator response: Notify the security administrator.

RACF Security Administrator Response: Define the correct profile to the OPERCMDS class.

Destination: Descriptor code is 6.

IRRB076I RESTART CONNECTION NODE IN PROGRESS FOR LOCAL NODE.

Explanation: A restart connection for the local node was initiated.

System action: RACF restarts the connection for local node services.

Operator response: None.

Destination: Descriptor code is 6. Routing code is 2.

IRRB077I SYSNAME SHOULD NOT BE SPECIFIED WHEN NODE(*) IS SPECIFIED ON THE RESTART COMMAND.

Explanation: When specifying NODE(*) to restart
connections to all nodes, a specific SYSNAME cannot be specified.

**System action:** The RESTART command is ignored.

**Operator response:** Correct and reissue the command. You can enter NODE(*) SYSNAME(*) or NODE(node-name) SYSNAME(system-name).

**Destination:** Descriptor code is 6.

<table>
<thead>
<tr>
<th>IRRB078I</th>
<th>RRSF NODE node-name IS A SINGLE-SYSTEM NODE AND THE SYSNAME PARAMETER SHOULD NOT BE SPECIFIED.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> RRSF node node-name is a single-system node and the SYSNAME keyword cannot be specified.</td>
<td></td>
</tr>
<tr>
<td><strong>System action:</strong> The RESTART command is ignored.</td>
<td></td>
</tr>
<tr>
<td><strong>Operator response:</strong> Correct and reissue the command.</td>
<td></td>
</tr>
<tr>
<td><strong>Destination:</strong> Descriptor code is 6.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IRRB079I</th>
<th>RRSF NODE node-name IS A MULTISYSTEM NODE AND THE SYSNAME PARAMETER SHOULD BE SPECIFIED.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> When NODE node-name is specified, the SYSNAME() keyword is mandatory in order to RESTART the connection to a specific system in the multisystem node.</td>
<td></td>
</tr>
<tr>
<td><strong>System action:</strong> The RESTART command is ignored.</td>
<td></td>
</tr>
<tr>
<td><strong>Operator response:</strong> To restart connections to all systems within a multisystem node, specify NODE(node-name) SYSNAME(*) on the RESTART command. To restart the connection to a specific system within a multisystem node, specify NODENAME(node-name) SYSNAME(system-name).</td>
<td></td>
</tr>
<tr>
<td><strong>Destination:</strong> Descriptor code is 6.</td>
<td></td>
</tr>
</tbody>
</table>

| IRRB080I | RRSF NODE(S) WITH CONNECTION STATUS OF [DEFINED | DORMANT] WILL NOT BE RESTARTED. |
|----------|--------------------------------------------------------------------------------|
| **Explanation:** RRSF nodes in the DEFINED or DORMANT state do not have an existing conversation and does not restart. |
| **System action:** RESTART CONNECTION to nodes in the DEFINED or DORMANT state are ignored. The command continues processing nodes in other states. |
| **Operator response:** None. |
| **Destination:** Descriptor code is 6. |

<table>
<thead>
<tr>
<th>IRR081I</th>
<th>INCORRECT RRSF NODE NAME ENTERED ON THE RESTART COMMAND.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> An RRSF node name with an incorrect length was entered on the RESTART CONNECTION command. The node name must be 1 to 8 characters.</td>
<td></td>
</tr>
<tr>
<td><strong>System action:</strong> The RESTART command is not processed.</td>
<td></td>
</tr>
<tr>
<td><strong>Operator response:</strong> Reissue the RESTART command by using a valid node name.</td>
<td></td>
</tr>
<tr>
<td><strong>Destination:</strong> Descriptor code is 6.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IRR082I</th>
<th>INCORRECT SYSNAME ENTERED ON THE RESTART COMMAND.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> A system name with an incorrect length was entered on the RESTART CONNECTION command. The system name must be 1 to 8 characters.</td>
<td></td>
</tr>
<tr>
<td><strong>System action:</strong> The RESTART command is not processed.</td>
<td></td>
</tr>
<tr>
<td><strong>Operator response:</strong> Reissue the RESTART command by using a valid system name.</td>
<td></td>
</tr>
<tr>
<td><strong>Destination:</strong> Descriptor code is 6.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IRR001I</th>
<th>MAXIMUM NUMBER nn OF COMMAND TASKS EXCEEDED FOR subsystem SUBSYSTEM. LAST COMMAND IGNORED.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> The RACF subsystem allows nn simultaneously active command-processing modules and ignores all requests in excess of this number. This message is not issued on systems running RACF version 2 release 2 or the z/OS Security Server.</td>
<td></td>
</tr>
<tr>
<td><strong>System action:</strong> The RACF subsystem continues operation.</td>
<td></td>
</tr>
<tr>
<td><strong>Operator response:</strong> Reenter the command.</td>
<td></td>
</tr>
<tr>
<td><strong>Problem Determination:</strong> None.</td>
<td></td>
</tr>
<tr>
<td><strong>Destination:</strong> Descriptor code is 6. Routing code is 2.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IRR002I</th>
<th>subsystem SUBSYSTEM COMMAND SCAN ERROR. CODE IS cde-rc.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> The TSO command scan service failed with return code cde, reason code rc.</td>
<td></td>
</tr>
<tr>
<td><strong>System action:</strong> RACF subsystem subsystem stops.</td>
<td></td>
</tr>
<tr>
<td><strong>Operator response:</strong> Report the complete text of this message to your system programmer.</td>
<td></td>
</tr>
<tr>
<td><strong>System programmer response:</strong> Determine the cause of the command scan error.</td>
<td></td>
</tr>
<tr>
<td><strong>Problem Determination:</strong> None.</td>
<td></td>
</tr>
<tr>
<td><strong>Destination:</strong> Descriptor code is 6. Routing code is 2.</td>
<td></td>
</tr>
</tbody>
</table>
IRRC003I  COMMAND command-name IS NOT VALID.
Explanation: Command command-name is not syntactically correct.
System action: The RACF subsystem ignores the request and continues operation.
Operator response: Reenter the command with the correct syntax.
Problem Determination: None.
Destination: Descriptor code is 6. Routing code is 2.

IRRC004I  COMMAND cccccccc IS NOT SUPPORTED.
Explanation: The RACF subsystem does not support the entered command.
System action: The RACF subsystem ignores the request and continues operation.
Operator response: None.
Problem Determination: None.
Destination: Descriptor code is 6. Routing code is 2.

IRRC005I  UNABLE TO LOAD MODULE module-name FOR subsystem SUBSYSTEM. COMMAND NOT EXECUTED.
Explanation: Command module module-name could not be loaded.
System action: The RACF subsystem ignores the request and continues operation.
Operator response: None.
Problem Determination: None.
Destination: Descriptor code is 6. Routing code is 2.

IRRC006I  subsystem SUBSYSTEM COMMAND HANDLING TASK TERMINATED IN ABEND PROCESSING.
Explanation: The indicated subsystem command-handling task experienced an abend during the handling of a previously encountered abend.
System action: The indicated subsystem detaches the abending command-processing task and attempts to reattach the task. If the task continues to abend, the task permanently remains detached and the address space continues operation.
Operator response: Report the exact text of this message to your system programmer.
System programmer response: Examine abend dumps and fix the problem before the next IPL.

IRRC007I  ROUTE OF RACF command COMMAND TO MULTIPLE SYSTEMS IS NOT SUPPORTED. REISSUE THE COMMAND TO A SINGLE SYSTEM ONLY.
Explanation: The RACF command was prefixed with the MVS ROUTE command, directing the command to multiple members of a sysplex. This is allowed only for the RACF DISPLAY, SIGNOFF, and RVARY commands and only when no RVARY keyword other than LIST is specified, either explicitly or by default. The RACF command must be reissued to a single member only.
System action: The RACF subsystem ignores the request and continues operation.
Operator response: Reissue the command to a single member.
Problem Determination: None.
Destination: Descriptor code is 6. Routing code is 2.

IRRC010I  UNABLE TO ESTABLISH RACF ENVIRONMENT FOR COMMAND command.
Explanation: The command running in the RACF subsystem address space did not run because the appropriate security environment was not established.
System action: The resources associated with running the failed command are released and the subsystem proceeds with the next command request, if any.
Operator response: If available, check the RACROUTE return and reason codes from the following IRRC011I, IRRC012I, or IRRC021I messages for corrective action. If RACROUTE ended abnormally, message ICH409I contains information that can be used for problem determination and corrective action.
Problem Determination: None.
Destination: Descriptor code is 6.

Explanation: A RACROUTE REQUEST=VERIFY was used to create the security environment required to run one of the following in the RACF subsystem address space:
- A directed command
- An automatically directed command
- An automatically directed password
- A password synchronization request
- An automatically directed application update

The RACROUTE failed.
**System action:** The resources associated with running the failed command are released and the subsystem proceeds with the next command request, if any.

**Operator response:** Check the RACROUTE REQUEST=VERIFY return and reason codes in z/OS Security Server RACROUTE Macro Reference for an explanation of the codes.

**Note:** The reason and return codes in this message are displayed in decimal format. The codes presented in z/OS Security Server RACROUTE Macro Reference are shown in hexadecimal format.

The RACROUTE return code is also called the SAF return code.

**Destination:** Descriptor code is 6.

---

**IRRC012I** TARGET USER ID node.userid DOES NOT EXIST.

**Explanation:** The RACF subsystem address space attempted to issue one of the following on behalf of the named user, but the user is not defined to RACF:

- A directed command
- An automatically directed command
- An automatically directed password
- A password synchronization request
- An automatically directed application update

This message is issued with IRRC010I.

**System action:** Command processing fails to complete.

**User response:** If the command was a directed command from another node, the command issuer should correct the user name in the AT keyword. If the command was an automatically directed command from another node, contact your RACF security administrator.

**RACF Security Administrator Response:** Ensure that matching user IDs exist on nodes participating in automatic command direction processing.

**Destination:** Descriptor code is 6. Routing code is 2.

---

**IRRC013I** Password synchronized successfully for source-userid at source-node and target-userid at target-node.

**Explanation:** A password synchronization request that was originated by the source user ID has been completed for the target user ID. This is an informational message. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

**System action:** The system continues processing.

**System programmer response:** The return code indicated in this message reflects the return code from the MVS IEFSSREQ subsystem interface. The return code may be one of these values:

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>The subsystem does not support this function.</td>
</tr>
<tr>
<td>8</td>
<td>The subsystem exists, but is not active.</td>
</tr>
<tr>
<td>12</td>
<td>The subsystem is not defined in the IEFSSNxx parmlib member.</td>
</tr>
<tr>
<td>16</td>
<td>The function has not completed. This is a disastrous error.</td>
</tr>
<tr>
<td>20</td>
<td>The SSOB or SSIB have lengths or formats that are not valid.</td>
</tr>
<tr>
<td>24</td>
<td>The SSI has not been initialized.</td>
</tr>
</tbody>
</table>

A return code of 4, 16, 20 or 24 indicates a RACF code problem. Report this message to the IBM support center.

A return code of 8 or 12 indicates an installation or RACF subsystem configuration problem. See z/OS Security Server RACF System Programmer's Guide for configuration considerations for the RACF subsystem.
IRRC016I • IRRC021I

IRRC016I  User ID userid is not defined to use a password.

Explanation:  RACF password synchronization attempted to process a password change request for a user. The user ID in the message is not required to enter a password, but is identified by way of an OIDCARD. RACF password synchronization is not applicable to the user ID in this message. This is an informational message. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

User response:  If you do not want to see this message every time the associated user ID changes their password, either disable password synchronization for the user who initiated the password change, or have the security administrator alter this user ID profile to require a password by using the ALTUSER command.

IRRC017I  Unable to verify PWSYNC association with userid userid.

Explanation:  RACF attempted to verify the RACF association with the user ID shown in the message. The verification attempt was not successful. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

User response:  Use the RACLINK LIST command to list the associations for the user ID in the message to determine the nature of the failure, or report this message to your administrator.

IRRC018I  Unable to set password date. Return code is return-code. Reason code is reason-code.

Explanation:  RACF attempted to propagate an update to the PASSDATE field of the RACF user profile identified in the user's RRSFLIST data set, but was unable to complete the update. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System action:  The PASSDATE field of the user profile was not updated. The system continues processing.

User response:  Examine the return and reason codes to determine the nature of the problem. The return and reason codes displayed in this message have been returned from the RACF database manager. For a description of the RACF manager return codes, see "RACF manager return codes" on page 405.

IRRC020I  Passdate was set for userid at node-name.

Explanation:  RACF has successfully updated only the password change date in the specified user ID profile. This is an informational message. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

User response:  None required.

IRRC021I  ACCESS HAS BEEN REVOKED FOR USER ID userid.

Explanation:  The RACF subsystem address space attempted to issue one of the following on behalf of the indicated user ID, but that user ID's access has been revoked:

• A directed command
• An automatically directed command
• An automatically directed password
• A password synchronization request
• An automatically directed application update

This message is issued with IRRC010I. It is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

System action:  The command being processed is unsuccessful; processing ends.

User response:  Verify that the user ID specified is correct. If it is, contact the RACF security administrator.

RACF Security Administrator Response:  A command has been directed either manually or automatically to a user ID whose access has been revoked. Take whatever action the site RACF security policy requires for requests made on behalf of revoked users.
IRRC022I  RACF REMOTE SHARING  
CONNECTION TO NODE node-name  
[SYSNAME system-name] HAS  
CHANGED FROM [OPERATIVE  
ACTIVE | OPERATIVE PENDING  
CONNECTION | OPERATIVE  
PENDING VERIFICATION] TO  
OPERATIVE ERROR. FAILURE  
OCCURRED WHEN APPC VERB verb  
WAS ISSUED. RETURN CODE = {APPC  
RETURN-CODE | NOT RESPONDING}  

Explanation: The local RACF RRSF node is unable to  
communicate with the indicated node. The state of the  
connection has been changed to operative error. If  
SYSNAME information is present in this message, the  
node node-name is a multisystem node.  

System action: The RACF subsystem address space  
saves the request that was issued and when the  
problem has been corrected, RACF sends the request to  
the indicated node.  

Operator response: See z/OS MVS Programming  
Writing Transaction Programs for APPC/MVS for  
information about the APPC verb and return code to  
determine the cause of the communication failure.  
Correct the problem and restart the connection by  
using the TARGET command.  

Destination: Descriptor code is 4. Routing codes are 2  
and 9.  

IRRC023I  RACF REMOTE SHARING SERVER  
COULD NOT BE REGISTERED TO  
APPC/MVS. FAILURE OCCURRED  
WHEN APPC VERB verb WAS ISSUED.  
RETURN CODE = {APPC  
RETURN-CODE | NOT RESPONDING}  
REASON CODE = {APPC REASONCODE}  

Explanation: The local RACF remote sharing  
service (RRSF) was unable to establish itself as an  
APPC/MVS server. The specific APPC/MVS verb did not  
complete successfully. Failure occurred when the  
APPC/MVS verb was issued. Correct the problems and  
issue the TARGET command to make the local node  
operative.  

System action: The RACF subsystem address space  
cannot send or receive any remote sharing requests.  

Operator response: Check the status of the connection  
by using the TARGET command on both the local and  
remote node. Issue the appropriate TARGET commands  
to place the connection into the state you want. If the  
two nodes are not in the required state, see z/OS MVS  
Programming: Writing Transaction Programs for  
APPC/MVS to determine why RACF was unable to  
successfully execute the APPC/MVS verb. Correct the  
problems and issue the TARGET command to make the  
local node operative.  

Destination: Descriptor code is 4. Routing codes are 2  
and 9.  

IRRC024I  RACF REMOTE SHARING  
CONNECTION TO NODE node-name  
[SYSNAME system-name] DID NOT  
COMPLETE SUCCESSFULLY. FAILURE  
OCCURRED WHEN APPC VERB verb  
WAS ISSUED. RETURN CODE = {APPC  
RETURN-CODE}  

Explanation: The local RACF RRSF connection to a  
remote RACF RRSF node was unable to successfully  
execute an APPC/MVS verb. Here are some typical  
causes:  
- VTAM® or APPC is not active on the local or remote  
node.  
- VTAM or APPC has been unable to connect to the  
server on the remote node.  
- A TARGET command has not been issued to make  
the remote node OPERATIVE.  
- The appropriate RACF security definitions have not  
been provided.  

If SYSNAME information is present in this message,  
the node node-name is a multisystem node.  

System action: The RACF subsystem address space  
cannot send or receive any remote sharing requests  
to the remote node.  

Operator response: Check the status of the connection  
by using the TARGET command on both the local and  
remote node. Issue the appropriate TARGET commands  
to place the connection into the state you want. If the  
two nodes are not in the required state, see z/OS MVS  
Programming: Writing Transaction Programs for  
APPC/MVS to determine why RACF was unable to  
successfully execute the APPC/MVS verb. Correct the  
problems and issue the TARGET command to make the  
local node operative.  

Destination: Descriptor code is 4. Routing codes are 2  
and 9.  

IRRC025I  RACF REMOTE SHARING SERVER  
COULD NOT BE REGISTERED TO  
APPC/MVS IN THE ALLOTED TIME  
INTERVAL. FAILURE OCCURRED  
WHEN APPC VERB verb WAS ISSUED.  

Explanation: The RACF remote sharing facility (RRSF)  
could not be registered as an APPC/MVS server. The  
specific APPC/MVS verb did not complete within  
30 minutes.  

System action: RRSF is unable to make any new
connections to other remote RRSF nodes. Work for the remote nodes is being queued until they can be activated.

**Operator response:** See [z/OS MVS Programming](#) **Writing Transaction Programs for APPC/MVS** on isolating the cause of the communication failure. Correct the problems and restart the connection using the TARGET command.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.

---

**IRRC026I**

**RACF REMOTE SHARING REQUEST TO NODE node-name [SYSNAME system-name] COULD NOT BE COMPLETED IN THE ALLOTTED TIME INTERVAL. FAILURE OCCURRED WHEN THE APPC VERB verb WAS ISSUED.**

**Explanation:** The local RACF RRSF node is unable to complete a request to the indicated node. If SYSNAME information is present in this message, the node node-name is a multisystem node. This message goes to the SYSLOG and is accompanied by other messages.

**System action:** The RACF subsystem address space saves the request that was issued and when the connection has been made, RACF sends the request to the indicated node.

---

**IRRC028I**

**RACF REMOTE SHARING SERVER HAS DE-REGISTERED FROM APPC/MVS.**

**Explanation:** The RACF address space has registered as an APPC/MVS server when the appropriate TARGET command was issued. This registration is being ended by either a request (TARGET, RESTART CONNECTION, or STOP) sent by a person or by the RACF remote sharing facility (RRSF) because of a failure within the subsystem.

**System action:** The RACF subsystem stops processing APPC/MVS allocate requests from other RRSF nodes.

**Operator response:** When it is appropriate for RRSF to accept APPC/MVS allocate requests from another node, issue the appropriate TARGET commands.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.

---

**IRRC029I**

**RACF REMOTE SHARING MODULE module-name HAS EXPERIENCED A FAILURE WITH THE VSAM FILE data-set-name. IRRSSQ00 REQUEST = request, IRRSSQ00 RETURN CODE = module-return-code, GRS RETURN CODE = GRS-return-code.**

**Explanation:** RACF remote sharing experienced a failure when it attempted to checkpoint a request to a specific VSAM file. The IRRSSQ00 REQUEST is either:

- R - read
- X - read_next
- I - insert
- E - erase

The IRRSSQ00 RETURN CODE indicates either a logic or a GRS failure:

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ACB pointer or DSNAME not set in the node definition block</td>
</tr>
<tr>
<td>2</td>
<td>ENQ</td>
</tr>
<tr>
<td>3</td>
<td>Unknown request type</td>
</tr>
<tr>
<td>D</td>
<td>DEQ</td>
</tr>
</tbody>
</table>

The GRS RETURN CODE definitions can be found in [z/OS MVS Programming: Authorized Assembler Services Reference ALE-DYN](#) or [z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG](#). If the IRRSSQ00 RETURN CODE is either 1 or 3, the GRS RETURN CODE is set to zero and should be ignored.

**System action:** The RACF subsystem address space is not able to send or receive remote sharing requests for the specified node.

**Operator response:** Determine why RACF remote sharing experienced the failure when checkpointing information to the VSAM file. Check for other instances of either this message, or message IRRC029I, and LOGRECs. A ‘d grs,res=(syszrac3,*)’ may be issued from the MVS master console for major name SYSZRA3 ENQ information. A ‘d grs,c’ issued from the MVS master console may be used to display all outstanding resource contention. If the IRRSSQ00 RETURN CODE is either 1 or 3, report this problem to the IBM support center. Correct the problems. When the problem is resolved, start the node using the TARGET command (for example, TARGET NODE(x) OPERATIVE ...).

**Destination:** Descriptor code is 6. Routing code is 2.

---

**IRRC030I**

**RACF REMOTE SHARING MODULE module-name HAS EXPERIENCED A FAILURE WITH THE VSAM FILE data-set-name. IRRSSQ00 REQUEST = request, IRRSSQ00 RC = module-return-code, VSAM RC = vsam-return-code, SHOWCB RC = showcb-return-code, VSAM REASON CODE = vsam-reason-code.**

**Explanation:** RACF remote sharing experienced a failure when it attempted to checkpoint a request to a specific VSAM file. The IRRSSQ00 REQUEST is either:

- R - read
- X - read_next

The IRRC030I RETURN CODE indicates either a logic or a GRS failure:
The IRRSSQ00 RETURN CODE indicates a VSAM failure:

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>MODCB RPL ACB</td>
</tr>
<tr>
<td>5</td>
<td>MODCB RPL AREA</td>
</tr>
<tr>
<td>6</td>
<td>MODCB RPL RECLN</td>
</tr>
<tr>
<td>7</td>
<td>MODCB RPL ARG</td>
</tr>
<tr>
<td>8</td>
<td>MODCB RPL OPTCD=NUP</td>
</tr>
<tr>
<td>9</td>
<td>GET</td>
</tr>
<tr>
<td>A</td>
<td>PUT</td>
</tr>
<tr>
<td>B</td>
<td>ERASE</td>
</tr>
<tr>
<td>C</td>
<td>ENDRQ</td>
</tr>
<tr>
<td>E</td>
<td>OPEN</td>
</tr>
</tbody>
</table>

The VSAM RETURN CODE, SHOWCB RETURN CODE, and VSAM REASON CODE definitions may be found in [z/OS DFSMS Macro Instructions for Data Sets]. If the SHOWCB RETURN CODE is non-zero, the value for the VSAM REASON CODE should be ignored.

**System action:** The RACF subsystem address space is not able to send or receive remote sharing requests for the specified node.

**Operator response:** Determine why RACF remote sharing experienced the failure when checkpointing information to the VSAM file. Typical causes of this problem are the VSAM file is full or the disk containing the VSAM file is experiencing I/O errors. Check for other instances of either this message, or message IRRC029I, and LOGRECs. Correct the problems. When the problem is resolved, start the node by using the TARGET command (for example, TARGET NODE(x) OPERATIVE ...).

**Destination:** Descriptor code is 6. Routing code is 2.

---

**IRR032I**  
RACF REMOTE SHARING  
CONNECTION TO NODE node-name  
[SYSNAME system-name] HAS  
CHANGED FROM [DORMANT LOCAL | DORMANT BY MUTUAL REQUEST] TO DORMANT ERROR.

**Explanation:** The local RACF remote sharing facility (RRSF) node is unable to checkpoint RRSF requests for the indicated node. A VSAM file used to checkpoint requests is not functional. If SYSNAME information is present in this message, node node-name is a multisystem node.

**System action:** The RACF subsystem stops all processing for this node until the problem with the VSAM file is resolved.

**Operator response:** See the VSAM documentation on isolating the cause of the VSAM failure. RACF message IRRC029I or IRRC030I contains the return and reason codes describing the VSAM failure. Correct the problems and redefine the VSAM files by using the TARGET command.

**Destination:** Descriptor code is 6. Routing code is 2.

---

**IRR033I**  
RACF REMOTE SHARING  
CONNECTION TO NODE node-name  
[SYSNAME system-name] HAS  
CHANGED FROM [OPERATIVE ACTIVE | OPERATIVE PENDING CONNECTION | OPERATIVE PENDING VERIFICATION | DORMANT REMOTE] TO OPERATIVE ERROR.

**Explanation:** The local RACF remote sharing facility (RRSF) node is unable to send an RRSF request to the indicated node. The VSAM file used to checkpoint requests is the most likely cause of the problem. If SYSNAME information is present in this message, the node node-name is a multisystem node.

**System action:** The RACF subsystem stops all processing for this node until the problem is resolved.

**Operator response:** Review the system log for accompanying messages. If the problem was caused by the VSAM file, see the VSAM documentation on isolating the cause of the VSAM failure. RACF message IRRC030I or IRRC031I contains the VSAM return and reason codes describing the VSAM failure. Correct the problems and redefine the VSAM files by using the TARGET command.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.

---

**IRR031I**  
SUBSYSTEM DATA SET data-set-name IS FULL.

**Explanation:** The indicated workspace data set on the indicated subsystem is full.

**System action:** Processing for this directed or RACLINK command stops.

**Operator response:** Contact your system programmer or data management expert.

**System programmer response:** Allocate a larger VSAM data set. See [z/OS Security Server RACF System Programmer’s Guide] for information about the procedure to follow.

**Destination:** Descriptor code is 6. Routing code is 2.
**IRRC034I** RACF IS UNABLE TO ESTABLISH A TSO I/O ENVIRONMENT FOR COMMAND command. TSO STACK HAS RETURNED A RETURN CODE OF return-code.

**Explanation:** The command running in the RACF subsystem address space did not run because the appropriate TSO I/O environment could not be established.

**System action:** The resources associated with the failed command are released and the subsystem proceeds with the next command request, if any.

**Operator response:** Report the exact text of this message to your system programmer.

**System programmer response:** Use the indicated TSO STACK return code to determine the cause of the condition and correct it. For an explanation of the return code, see z/OS TSO/E Programming Services.

**Destination:** Descriptor code is 6. Routing code is 2.

**IRRC035I** You have not been authorized for password synchronization.

**Explanation:** Your RACF user profile contains approved peer user ID associations with password synchronization with other user IDs. However, your RACF security administrator has not authorized your password changes to be synchronized by RACF. This message is appended to the user’s RRSFLIST data set. If the data set is full, this message is transmitted to the user’s TSO terminal.

**System action:** Your RACF password has been changed only in your RACF user profile.

**User response:** Report this message to your RACF security administrator.

**System programmer response:** If appropriate, give the user READ access to the PWSYNC profile in the RRSFDATA class.

**Problem Determination:** The ability to synchronize passwords is protected by way of RACF profiles in the RRSFDATA class. Ensure that the RRSFDATA class is active, profiles are up to date (that is, RACLIST REFRESH if you have the class RACLISTed), and that you have the proper authority granted to the profile covering the PWSYNC entity. See z/OS Security Server RACF Security Administrator's Guide for more details.

**IRRC036I** This password synchronization request was originated by userid at node-name.

**Explanation:** RACF has processed a password synchronization request that was originated on your behalf by the user ID specified in the message. This message is appended to the user’s RRSFLIST data set. If the data set is full, this message is transmitted to the user’s TSO terminal.

**User response:** No action required. This is an informational message.

**IRRC037I** AN AUTOMATIC PASSWORD DIRECTION REQUEST COULD NOT BE PERFORMED. RACROUTE RETURN CODE IS saf-return-code, RACF RETURN CODE IS return-code, RACF REASON CODE IS reason-code. USER userid NOT PROCESSED.

**Explanation:** A password synchronization request could not be performed. RACF encountered an error on a RACROUTE REQUEST=VERIFY statement. This message is appended to your RRSFLIST data set.

**User response:** Report this message to your RACF system programmer.

**System programmer response:** Check the RACROUTE REQUEST=VERIFY return and reason codes (in hexadecimal) in z/OS Security Server RACROUTE Macro Reference for an explanation of the codes. The RACROUTE return is also called the SAF return code.

**IRRC038I** A request to process Kerberos key information for user user failed. Processing continues.

**Explanation:** An error occurred while attempting to generate a Kerberos key for a user password change.

**System action:** All processing except for the key update is completed.

**User response:** Report this message to the system programmer and provide the exact text of the message.

**System programmer response:** Use the RLIST command to list the KERBDFLT profile definition of the local Kerberos realm in the REALM class and verify that the local realm name (KERBNAME) is defined. Use the LISTUSER command to list the KERB segment information for this user and verify that this information may be accessed. Correct any problems and ask the user to do another password change.

**IRRC039I** A PASSWORD SYNCHRONIZATION REQUEST COULD NOT BE PERFORMED. RACROUTE RETURN CODE IS saf-return-code, RACF RETURN CODE IS return-code, RACF REASON CODE IS reason-code. USER userid NOT PROCESSED.

**Explanation:** The password or password phrase for the user ID was changed; however, password synchronization for the other user IDs associated with user ID could not be processed. User ID has RACLINK associations with one or more other user IDs; the other user IDs were not updated. RACF has encountered an...
IRRC040I  •  IRRC052I

error during RACROUTE processing. This message is appended to your RRSFLIST data set.

User response: Report this message to your RACF system programmer.

System programmer response: Check the RACROUTE REQUEST=VERIFY return and reason codes in /z/OS Security Server RACROUTE Macro Reference for an explanation of the codes. The RACROUTE return is also called the SAF return code.

---

IRRC040I  RACF REMOTE SHARING CANNOT COMMUNICATE USING THE TCP PROTOCOL. THE RACF SUBSYSTEM RUNNING UNDER USER ID user IS NOT RUNNING AS A Z/OS UNIX PROCESS.

Explanation: The local RACF remote sharing node could not open a socket to communicate over the TCP protocol because the RACF subsystem is not running as a z/OS UNIX process. The most likely cause of this failure is that the subsystem address space identity user does not have an OMVS segment. Message IRRB023I is issued before IRRC040I, and it contains details of the service that failed when trying to establish a z/OS UNIX environment.

System action: The local socket listener for TCP was not established, and remote sharing is unable to communicate with any node that requires TCP.

RACF Security Administrator Response: See message IRRB023I for information about how to resolve the problem.

System programmer response: After the problem is resolved, use the TARGET command to make the local node OPERATIVE, and then do the same for all remote nodes that use TCP as the transport protocol. Note the entire subsystem does not need to be stopped and restarted.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

---

IRRC051I  RACF REMOTE SHARING TCP LISTENER TASK STARTING.

Explanation: This is an informational message that is written to the SYSLOG after the program that listens for connections from remote TCP nodes has completed its initialization. Note this task is always started. Message IRRC054I is issued when the listener socket is established as a result of defining TCP information for the local node and making it operative.

---

IRRC052I  RACF REMOTE SHARING CONNECTION TO NODE node-name [SYSNAME system-name] COULD NOT BE ESTABLISHED. FAILURE OCCURRED WHEN SERVICE service-name WAS ISSUED. RETURN CODE = return-code REASON CODE = reason-code DIAGNOSTIC CODE = diag-code.

Explanation: RACF encountered an unexpected return code while starting one of the z/OS UNIX System Services required in order to establish a connection to the socket listener on the remote node because a remote node or system specifying the TCP protocol was attempting to be OPERATIVE.

System action: If you can try the error again, the RRSF connection to the node goes into the OPERATIVE PENDING CONNECTION state and RRSF periodically attempts to establish the connection. If a subsequent connection attempt fails, this message is only issued if it fails for a different reason. If you cannot try the error again, the RRSF connection to the node goes into the OPERATIVE PENDING VERIFICATION state and RRSF does not attempt to establish the connection again.

System programmer response: Look up the return (errno) and reason code (errnojr) in /z/OS UNIX System Services Messages and Codes. When looking up the reason code, use only the low-order halfword of the displayed value. There is a name and a value for each return code. For more information about the identified service service-name, see /z/OS UNIX System Services Programming: Assembler Callable Services Reference and look for common errors, by name, that include possible causes. Your network administrator might be able to help you. If you are not able to determine the problem, contact IBM service.

Destination: Descriptor code is 4. Routing codes are 2 and 9.
IRRC053I • IRRC057I

up the reason code, use only the low-order halfword of
the displayed value. There is a name and a value for
each return code. For more information about the
identified service service-name, see z/OS UNIX System
Services Programming: Assembler Callable Services
Reference and look for common errors, by name, that
include possible causes. Your network administrator
might be able to help you. If you are not able to
determine the problem, contact IBM service.

An error with the BPX1RCV service can indicate a
problem with AT-TLS detected on the remote system.
Look for error messages on the console of the remote
system.

Destination: Descriptor code is 4. Routing codes are 2
and 9.

IRRC053I RACF REMOTE SHARING TCP
LISTENER TASK TERMINATING.

Explanation: This message is written to the SYSLOG
as the program that listens for connections from remote
TCP nodes stops processing. The program stops as a
result of an operator request to restart all connections
or to stop the RACF subsystem address space. The
program can also stop as the result of an internal error
(ABEND). Earlier messages might indicate the nature of
the problem.

IRRC054I RACF REMOTE SHARING TCP
LISTENER HAS BEEN SUCCESSFULLY
ESTABLISHED.

Explanation: When TCP protocol information is
specified for the local node, and the local node is made
OPERATIVE, RRSF establishes a socket listener on the
configured (or defaulted) IP address and port number.
This process has successfully initialized. This is an
informational message that is written to the console
and to SYSLOG.

System action: The TCP listener status becomes
ACTIVE. After this message has been issued, the
listener task starts the TCP connector task and then
waits for incoming TCP socket connections and other
RRSF and subsystem events, such as TARGET and
STOP commands.

Destination: Descriptor code is 4. Routing codes are 2
and 9.

IRRC055I RACF REMOTE SHARING TCP
LISTENER IS TERMINATING.

Explanation: The RACF address space has established
a TCP socket listener when the appropriate TARGET
command was issued. This process is being ended by
either a request (TARGET, RESTART CONNECTION,
or STOP) sent by a person or by the RACF remote
sharing facility (RRSF) because of a failure within the
subsystem.

System action: The TCP listener status becomes
INACTIVE. The RACF subsystem stops processing
socket connect requests from other RRSF nodes.
Existing TCP connections continue to function
normally.

Operator response: When it is appropriate for RRSF to
accept incoming TCP connect requests from another
node, issue the appropriate TARGET commands.

Destination: Descriptor code is 4. Routing codes are 2
and 9.

IRRC056I RACF REMOTE SHARING
CONNECTION TO NODE node-name
[SYSNAME system-name] HAS
ENCOUNTERED AN ERROR. FAILURE
OCCURRED WHEN SERVICE service
WAS ISSUED. RETURN CODE =
return-code REASON CODE = reason-code
DIAGNOSTIC CODE = diag-code.

Explanation: RRSF encountered an unexpected return
code while starting one of the services from z/OS
UNIX System Services that was used while
communicating with the remote node. If SYSNAME
information is present in this message, the node
node-name is a multisystem node.

System action: The RRSF connection to the node goes
into the OPERATIVE PENDING CONNECTION state
and RRSF periodically attempts to establish the
connection. A subsequent connection message indicates
whether the attempt is successful or not.

Operator response: If the connection is not
automatically reestablished, look up the return-code,
(errno) and reason-code (errnojr) in z/OS UNIX System
Services Programming: Assembler Callable Services
Reference and look for common errors, by name, that
include possible causes. Your network administrator
might be able to help you. If you are able to
correct the problem, make the connection operative by
using the TARGET command. If you are unable to
determine the problem, contact IBM service.

Destination: Descriptor code is 4. Routing codes are 2
and 9.

IRRC057I RRSF PROTOCOL CONVERSION
FROM old-protocol TO new-protocol FOR
NODE node-name [SYSNAME
system-name] HAS BEEN INITIATED.

Explanation: You have issued a TARGET command to
activate a new protocol for the specified remote
connection, for which a protocol instance exists.

System action: RRSF attempts to establish
communication under the new protocol. If successful, the old protocol is automatically disabled and deleted, and any existing requests queued in the workspace data sets of the old protocol are assumed by the new protocol.

Operator response: Monitor the connection to verify that the conversion process completes successfully. When the connection is established on the new protocol, see message IRRI027I (when new-protocol is TCP) or IRRI001I (when new-protocol is APPC). Then, when the workspace data sets for old-protocol are emptied, message IRRC058I is displayed. See the description of message IRRC058I for the action to take when it is issued. If the connection for new-protocol is not successfully established, see the error message that is issued for further instruction.

If you issued the TARGET command in error (perhaps you meant to define a new node instead of converting an existing one, but the node name is a typing error), then allow the conversion to complete. If it fails (perhaps because you have not specified correct protocol information, or have not completed network setup), you can then delete the new-protocol instance by using TARGET DELETE. If the conversion succeeds, you can then initiate the reverse conversion. No RRSF updates are lost.


Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRC059I RACF REMOTE SHARING

Connection to node-name [SYSNAME system-name] did not complete successfully. Remote node reports its state as state.

Explanation: When you attempt to establish communication with a remote node, the remote node responds to the connection request by communicating its current state. The state it reported is not a connectable state.

System action: On the local system, the state of the remote node is set to DORMANT-REMOTE, and there is no subsequent attempt to reconnect.

System programmer response: Log on to the remote node and issue the appropriate TARGET command or commands to fix the situation and, from that system, make the connection OPERATIVE.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRC060I RACF REMOTE SHARING

Connection to node-name [SYSNAME system-name] has encountered an error due to an improperly formatted message.

Explanation: While communicating with a remote node, the local node received a package of data with unexpected contents.

System action: The RACF subsystem address space changes the state of the connection to OPERATIVE PENDING CONNECTION and attempts to reestablish the connection. A subsequent connection message indicates whether the attempt is successful or not.

System programmer response: Attempt to reestablish communication by issuing the TARGET command with the OPERATIVE keyword from either side of the connection. If the problem persists, contact IBM service.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRC061I RACF REMOTE SHARING TCP

Listener has encountered an error. Failure occurred when service service was issued.

RETURN CODE = return-code REASON CODE = reason-code DIAGNOSTIC CODE = diag-code.
IRRC062I • IRRC080I

**Explanation:** While the RACF remote sharing TCP listener was listening for incoming connections, it encountered an error.

**System action:** The TCP listener status becomes INITIALIZING, and the listener attempts to reestablish itself.

**System programmer response:** Monitor the console to ensure that the listener successfully initializes. If it does not, look up the return (errno) and reason code (errnoj) in the z/OS UNIX System Services Messages and Codes. When looking up the reason code, use only the low-order halfword of the displayed value. There is a name and a value for each return code. For more information about the identified service service-name, see z/OS UNIX System Services Programming: Assembler Callable Services Reference. For more information about common errors, by name, that include possible causes.

Verify that TCP/IP and z/OS UNIX System Services are still active.

If the listener fails to reestablish itself, another error message is displayed. See that message for further action. If the problem persists, contact IBM service.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.

<table>
<thead>
<tr>
<th>IRRC062I</th>
<th>RACF REMOTE SHARING CONNECTION TO NODE node-name [SYSNAME system-name] CLOSED BY REQUEST OF THE REMOTE NODE.</th>
</tr>
</thead>
</table>

**Explanation:** This informational message indicates that the RRSF connection is closed intentionally as the result of an error, or as the result of a STOP, TARGET DORMANT, or RESTART command issued on the partner system. The message is also issued if the TARGET OPERATIVE command is specified when the connection is already OPERATIVE (this has essentially the same effect as RESTART). This message is only issued for TCP connections.

**System action:** The RACF subsystem address space changes the state of the connection to DORMANT-REMOTE. If the connection closed due to an error, a STOP, or a TARGET DORMANT, RACF does not attempt to establish the connection again. If the RESTART (or TARGET OPERATIVE) command is specified, the connection is established again, and appears as though it is a new connection. That is, you can expect to see message IRRI027I if the connection is successful.

**Operator response:** None. The connection must be established again from the system that closed it. If a RESTART or TARGET OPERATIVE command was issued, the attempt to reestablish the connection has been made.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.

<table>
<thead>
<tr>
<th>IRRC063I</th>
<th>RACF REMOTE SHARING TCP LISTENER COULD NOT BE STARTED IN THE ALLOTTED TIME INTERVAL.</th>
</tr>
</thead>
</table>

**Explanation:** The RACF remote sharing facility (RRSF) was unable to establish the TCP listener. It continually attempts to start the listener for approximately 30 minutes before giving up. Message IRRC050I, which was issued before this message, contains information about the nature of the failure.

**System action:** The TCP listener status becomes INACTIVE. RRSF is unable to communicate with remote RRSF nodes that use the TCP protocol. Work for the remote nodes is being queued until they can be activated.

**Operator response:** Correct the problems documented in message IRRC050I and restart the listener by making the local node operative again by using the TARGET command.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.

<table>
<thead>
<tr>
<th>IRRC064I</th>
<th>RACF REMOTE SHARING CONNECTION TO REMOTE NODE node-name [SYSNAME system-name] COULD NOT BE ESTABLISHED IN THE ALLOTTED TIME INTERVAL.</th>
</tr>
</thead>
</table>

**Explanation:** The RACF remote sharing facility (RRSF) was unable to establish a connection to remote node node-name. It continually attempts to connect for approximately 30 minutes before giving up. If SYSNAME information is present in this message, the node node-name is a multisystem node. Message IRRC056I, which was issued before this message, contains information about the nature of the failure.

**System action:** The remote node is put into the DORMANT-REMOTE state. Work for the remote node is being queued until it can be activated.

**Operator response:** Correct the problems documented in message IRRC056I and restart the connection by making the remote node operative again by using the TARGET command.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.

<table>
<thead>
<tr>
<th>IRRC080I</th>
<th>SUBSYSTEM COMMAND HANDLING TASK ENCOUNTED AN ERROR. ABEND CODE IS abend-code.</th>
</tr>
</thead>
</table>

**Explanation:** The command handler task was scheduling the running of a RACF command. This message appears when an abnormal event occurs. It is written to the SYSLOG.

**System action:** The command handler attempts to try the current work request again.
When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of ABEND, the subtask resumes processing any work in its input queue. See “Actions to Recover from an RRSF Failure” in z/OS Security Server RACF Diagnosis Guide for a complete discussion.

**Operator response:** Report the occurrence of the message to the system programmer.

**Problem Determination:** See z/OS MVS System Codes for an explanation of these codes.

**Destination:** Descriptor code is 6. Routing code is 2.

---

**IRRC081I**  
subsystem-name SUBSYSTEM COMMAND HANDLING TASK ENCOUNTERED AN ERROR. ABEND CODE IS abend-code. COMMAND HANDLING TASK ENDING.

**Explanation:** The COMMAND handler task was scheduling the running of a RACF command, a password change, or an application update in the RACF subsystem. This message appears when an abnormal event occurs.

**System action:** When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of ABEND, the subtask should resume processing any work in its input queue. See “Actions to Recover from an RRSF Failure” in z/OS Security Server RACF Diagnosis Guide for a complete discussion.

**Operator response:** Report the occurrence of the message to the system programmer.

**Problem Determination:** See z/OS MVS System Codes for an explanation of these codes. The task that started the COMMAND handling task attempts to restart the task. Verify that message IRRR020I was issued showing that the task was successfully restarted.

**Destination:** Descriptor code is 6. Routing code is 2.

---

**IRRC110I** Unable to establish RACF environment for application update request.

**Explanation:** The application update did not run in the RACF subsystem address space because the appropriate security environment was not established.

**System action:** The resources associated with running the failed update request are released and the subsystem proceeds with the next request, if any.

**User response:** For corrective action, check the RACROUTE return and reason codes from the IRRC011I, IRRC012I, or IRRC021I message that follows.

---

**IRRC130I** SYSTEM SSL FUNCTION x RETURNED ERROR CODE mnn DURING OPERATION NUMBER opcode WHILE PROCESSING THE [PASSWORD | PASS PHRASE] ENVELOPE FOR USER name.

**Explanation:** An unexpected error was detected when using System SSL functions to create a PKCS #7 envelope that contains the new password or password phrase for user name.

**System action:** The system continues processing.

**System programmer response:** Use the following table to identify the problem:

<table>
<thead>
<tr>
<th>x</th>
<th>System SSL function</th>
<th>mnn</th>
<th>Possible cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>'02'X</td>
<td>gsk_open_keyring</td>
<td>'03353009'X</td>
<td>IRR.PWENV.KEYRING not defined, or specified in incorrect case, or not owned by the RACF subsystem user ID</td>
</tr>
<tr>
<td>'03353017'X</td>
<td>The RACF subsystem does not have the trusted or privileged attribute, and does not have at least READ authority to IRR.DIGTCERT. LISTRING in the FACILITY class</td>
<td></td>
<td></td>
</tr>
<tr>
<td>'04'X</td>
<td>gsk_get_default_key</td>
<td>'0335300E'X</td>
<td>The certificate for RACF was not added to the key ring as the DEFAULT certificate</td>
</tr>
<tr>
<td>'03353026'X</td>
<td>A certificate was created without the KEYUSAGE value of HANDSHAKE,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>'03353033'X</td>
<td>No recipient certificates have been added to the key ring, or the certificates do not have TRUST status</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See if the source of the problem can be determined by reading the documentation for the failing API and return code in z/OS Cryptographic Services System SSL Programming. If the problem continues, contact your system support center.

If more diagnostic data is required, enable System SSL tracing by issuing the subsystem SET TRACE(SYSTEMSSL) command, then have the user attempt to change the password or password phrase again. System SSL trace records are created in a z/OS UNIX file named /tmp/gksssl.racf.pid.trc, where pid is the process identifier of the RACF task that invoked System SSL. Look for the trace record corresponding to the failing API. See z/OS Security Server RACF Command.
IRRC131I RACF ENCOUNTERED AN R_PROXYSERV ERROR WHILE ATTEMPTING TO CREATE AN LDAP CHANGE LOG ENTRY FOR AN UPDATE TO class name. SAF RETURN CODE=SAF-return-code, RACF RETURN CODE=return-code, RACF REASON CODE=reason-code.

Explanation: RACF attempted to create an LDAP change log entry for an update to name in the class class. The class name can be USER, GROUP, or CONNECT. If the Class name is CONNECT, then name takes the form of the user ID and the group name, separated by a period (for example IBMUSER.SYS1). The R_Proxyserv callable service (IRRSPY00) is used to communicate with LDAP. The service failed with the return codes shown. The LDAP change log entry was not created.

System action: The system continues processing.

System programmer response: Look up the return codes in z/OS Security Server RACF Callable Services and correct the problem.

Destination: Descriptor code is 6. Routing code is 2.

IRRC132I RACF ENCOUNTERED AN UNEXPECTED PARSE RETURN CODE mm WHILE PROCESSING AN IRRLOG00 COMMAND.

Explanation: While processing an update, RACF encountered return code mm from the IKJPARS service. This can happen when the RACFENVNT class is active, and RACF is either creating a PKCS #7 envelope for a user, or is attempting to create an LDAP change log entry. The IRRLOG00 command is created and sent to the RACF subsystem by the RACF database manager. The parse operation failed for this command. The profile being changed cannot be identified because the profile name is contained within the IRRLOG00 command.

System action: The profile was updated successfully on the RACF database, but the enveloping or change log operation did not occur. The system continues processing.

System programmer response: Contact the customer support center.

Destination: Descriptor code is 6. Routing code is 2.

IRRC133I RACF ENCOUNTERED INCORRECT APPLDATA SYNTAX IN THE [PASSWORD | PASSPHRASE].ENVELOPE PROFILE WHILE PROCESSING USER name DEFAULT VALUES ARE USED.

Explanation: While processing a password or password phrase update for user name, an error was encountered while interpreting the APPLDATA string in the RACFENVNT profile, which covers the resource identified in the message. The APPLDATA is used to specify the signing hash algorithm and encryption strength to use when building a PKCS #7 envelope for a user.

System action: RACF uses the default values of MD5 for the signing hash algorithm and triple DES for encryption.

RACF Security Administrator Response: Correct the APPLDATA. See z/OS Security Server RACF Security Administrator's Guide for details about defining the PASSWORD.ENVELOPE or PASSPHRASE.ENVELOPE resource. A generic profile might be used to cover either or both of these resources. This is indicated in the output of an RLIST command issued against the resource name.

Destination: Descriptor code is 6. Routing code is 2.

IRRC134I RACF ENCOUNTERED AN ICHEINTY ERROR WHILE ATTEMPTING TO PROCESS THE [PASSWORD | PASSPHRASE] ENVELOPE FOR USER name. OPERATION=optype, RETURN CODE=return-code, REASON CODE=reason-code.

Explanation: RACF attempted an ICHEINTY optype ('DELETE', 'STORE', or 'EXTRACT') on the PKCS#7 envelope for user name, but an unexpected error occurred. The contents of the envelope do not match the user's current password or password phrase.

System action: The system continues processing.

System programmer response: Make sure the RACF database templates are current. If this is not the problem, contact your customer support center.

Destination: Descriptor code is 6. Routing code is 2.

IRRC135I RACF ENCOUNTERED AN EXTRACT ERROR FOR PROFILE profile-name IN CLASS classname WHILE PROCESSING classname2 name. RETURN CODE=return-code, RACF RETURN CODE=racf-return-code, RACF REASON CODE=racf-reason-code.

Explanation: A RACROUTE REQUEST=EXTRACT was attempted but an unexpected return code was encountered. RACF was processing a change log.
request, or an enveloping request for the password or password phrase for user name. None of these functions succeeded.

Notes:
1. Because of an internal method being used, return-code is not a SAF return code found in z/OS Security Server RACROUTE Macro Reference (though racf-return-code and racf-reason-code match a documented combination).
2. For RACFEVNT class resources, profile-name might be a resource name that is covered by a generic profile. This is indicated in the output of an RLIST command issued against the resource name.

System action: The system continues processing.
System programmer response: Contact the customer support center.
Destination: Descriptor code is 6. Routing code is 2.


Explanation: A RACROUTE REQUEST=AUTH was attempted but an unexpected return code was encountered. RACF was attempting to check a user’s eligibility for PKCS #7 password or password phrase enveloping, by checking the user’s access to PASSWORD.ENVELOPE or PASSPHRASE.ENVELOPE in the RACFEVNT class. The user’s password or password phrase was not enveloped.

Note: Because of an internal method being used, return-code might not be a SAF return code found in z/OS Security Server RACROUTE Macro Reference (though racf-return-code and racf-reason-code match a documented combination).

System action: The system continues processing.
System programmer response: Contact the customer support center.
Destination: Descriptor code is 6. Routing code is 2.

IRRC137I  RACF RECEIVED CEEPIPI RETURN CODE rc FROM FUNCTION fcn WHILE PROCESSING USER name. CEEPIPI RESPONSE CODE hi-resp low-resp, REASON CODE hi-reas low-reas, FEEDBACK CODE hi-feed low-feed.

Explanation: An error was encountered during PKCS #7 envelope processing in the Language Environment interface used to set up the environment necessary for the execution of C language code. The function fcn identifies the internal C language function that was being invoked. The high-order four bytes and low-order four bytes of the response, reason, and feedback codes returned by CEEPIPI are displayed separately in hexadecimal. The user’s password or password phrase was not enveloped.

System action: The system continues processing.
System programmer response: Contact the customer support center.
Destination: Descriptor code is 6. Routing code is 2.

IRRC138I  RACF ENCOUNTERED AN UNEXPECTED PKCS#7 ENVELOPING ERROR WHILE PROCESSING USER name. R15=contents, OPERATION CODE=opcode, RC1=rc1, RC2=rc2, RC3=rc3.

Explanation: An unexpected error was encountered during PKCS #7 envelope processing for user name. The various diagnostic values are displayed. The user’s password or password phrase was not enveloped.

System action: The system continues processing.
System programmer response: Contact the customer support center.
Destination: Descriptor code is 6. Routing code is 2.

IRRC139I  THE NUMBER OF PASSWORD RECIPIENT CERTIFICATES ON IRR.PWENV.KEYRING EXCEEDS THE MAXIMUM OF 20. THE KEY RING IS OWNED BY THE RACF SUBSYSTEM ID user.

Explanation: A PKCS #7 password or password phrase envelope was being processed by the RACF subsystem in response to a request to the R_admin (IRRSEQ00) callable service. RACF only supports up to 20 recipients, each of which is identified by a certificate on the IRR.PWENV.KEYRING key ring. This key ring is owned by the identity under which the RACF subsystem is running, displayed in the message as user.

System action: The password or password phrase has been enveloped for only the first 20 certificates encountered (not including RACF’s certificate, which is the default certificate on the key ring). The system continues processing.

RACF Security Administrator Response: To avoid having this message displayed every time a password or password phrase envelope is requested, you can remove some certificates from the key ring by using the RACDCERT command. You can see the contents of the key ring by issuing the following command: RACDCERT ID(user) LISTRING(IRR.PWENV.KEYRING)
Note: The key ring name is case-sensitive, and so must be typed in uppercase.

Proper authority is required in order to issue this command. See z/OS Security Server RACF Command Language Reference for details about the RACDCERT command.

Destination: Descriptor code is 6. Routing code is 2.

IRRC144I THE [PASSWORD | PASS PHRASE] ENVELOPING FUNCTION CANNOT BE PERFORMED FOR USER user1. A PROPER UNIX SYSTEM SERVICES ENVIRONMENT DOES NOT EXIST FOR THE RACF SUBSYSTEM RUNNING UNDER USER ID user2.

Explanation: RACF attempted to build a PKCS #7 password or password phrase envelope for user ID user1, but was unsuccessful because the RACF subsystem is not running as a UNIX process. The most likely cause of this failure is one of the following causes:

1. The subsystem address space identity (identified in the message as user2) does not have an OMVS segment. In this case, message IRR8023I should have been issued during subsystem initialization.

2. An enveloping function was activated (by defining the PASSWORD.ENVELOPE or PASSPHRASE.ENVELOPE resource in the RACFEVNT class, and activating the class), but the RACF subsystem address space was not stopped and restarted.

System action: The enveloping function was not performed. The system continues processing.

RACF Security Administrator Response: In the case of number 1 above, define the RACF subsystem user ID as a z/OS UNIX user by defining an OMVS segment for its USER profile, and for its default group profile. See for more details about defining UNIX users. The RACF subsystem address space must be stopped and restarted after the OMVS information has been defined.

In the case of number 2 above, stop and restart the RACF subsystem address space. RACF recognizes that password or password phrase enveloping has been configured, and starts the proper UNIX services to dub itself as a UNIX process.

In order to avoid interruptions in services provided by the address space, it should be stopped during a period of low activity. See z/OS Security Server RACF System Programmer’s Guide for information about the RACF subsystem.

Destination: Descriptor code is 6. Routing code is 2.

IRRC143I RACF ENCONTERED AN EXTRACT ERROR: RETURN CODE=return-code, RACF RETURN CODE=racf-return-code, RACF REASON CODE=racf-reason-code, FOR PROFILE profile-name IN CLASS classname WHILE PROCESSING classname2 name.

Explanation: A RACROUTE REQUEST=EXTRACT was attempted but an unexpected return code was encountered. RACF was processing a change log request for the general resource profile name in class classname2.

Notes:
1. Because of an internal method being used, return-code is not a SAF return code found in z/OS Security Server RACROUTE Macro Reference (though racf-return-code and racf-reason-code match a documented combination).

2. This message ends with a period. This period is not part of the profile name.

System action: The system continues processing.

RACF Security Administrator Response: Contact the customer support center.

Destination: Descriptor code is 6. Routing code is 2.

IRRC144I RACF ENCOUNTERED AN R_PROXYSERV ERROR: SAF RETURN CODE=SAF-return-code, RACF RETURN CODE=return-code, RACF REASON CODE=reason-code, WHILE ATTEMPTING TO CREATE AN LDAP CHANGE LOG ENTRY FOR AN UPDATE TO class PROFILE name.

Explanation: RACF attempted to create an LDAP change log entry for an update to general resource profile name in the class. The R_Proxyserv callable service (IRRSPY00) is used to communicate with LDAP. The service failed with the return codes shown. The LDAP change log entry was not created.

Notes:
1. This message is like IRRC131I, which is issued for USER, GROUP, or CONNECT class profiles. In IRRC144I, the profile name starts on a separate line after the word "PROFILE". The profile name can span multiple lines depending on the profile name length.

2. This message ends with a period. This period is not part of the profile name.

System action: The system continues processing.

RACF Security Administrator Response: See the return codes in z/OS Security Server RACF Callable Services and correct the problem.

Destination: Descriptor code is 6. Routing code is 2.
IRRC313I  Pass phrase synchronized successfully for source-userid at source-node and target-userid at target-node.

Explanation: A password synchronization request for a password phrase that was originated by the source user ID has been completed for the target user ID. This is an informational message. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

IRRC318I  Unable to set pass phrase date. Return code is return-code. Reason code is reason-code.

Explanation: RACF attempted to propagate an update to the PHRDATE field of the RACF user profile identified in the user's RRSFLIST data set, but was unable to complete the update. This message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

User response: None required.

DISPLAY command messages

IRRD000I  DISPLAY ENCOUNTERED AN ERROR WHILE USING TSO PARSE, PARSE RETURN CODE WAS nn

Explanation: During the parse of the DISPLAY command image, the TSO parse facility returned a code that is documented in z/OS TSO/E Programming Services in the section containing information about IKJPARS.

System action: The DISPLAY command stops further processing and does not display any of the requested information.

Operator response: Verify that the DISPLAY command was correctly entered with the wanted keywords and associated operands. Reenter the command, and if the condition persists, notify your system programmer.

User response: See operator response.

System programmer response: See operator response.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRD001I  UNAUTHORIZED TO ISSUE THE DISPLAY COMMAND

Explanation: The user attempting to issue the DISPLAY command is not authorized to the proper profile in the OPERCMDS resource class.

System action: The DISPLAY command stops without further processing.

Operator response: Notify either the security administrator or the system programmer.

User response: See the operator response.

System programmer response: Either define the correct profile to the OPERCMDS class or notify the security administrator.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRD002I  NOT AUTHORIZED TO ISSUE THE DISPLAY COMMAND

Explanation: The user attempting to issue the DISPLAY command is not authorized to the proper profile in the OPERCMDS resource class.

System action: The DISPLAY command stops without further processing.

Operator response: Notify either the security administrator or the system programmer.

User response: See the operator response.

System programmer response: Either define the correct profile to the OPERCMDS class or notify the security administrator.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRD003I  DISPLAY COMMAND TERMINATED IN ABEND PROCESSING

Explanation: During the recovery processing of an abend condition another abend was detected.

System action: The DISPLAY command stops without further processing.
**Operator response:** Notify either the system programmer or the security administrator. Note whether the DISPLAY command provided any previous messages (such as IRRD080I), and whether a system dump has been taken.

**User response:** See the operator response.

**System programmer response:** Determine what keywords and operands are contained in the DISPLAY command. Examine the console log before this message for the presence of other messages that might provide further information. Also, examine the system dump data sets for the presence of a dump resulting from this condition.

**Destination:** Descriptor code is 1. Routing codes are 2 and 9.

---

**IRR004I** RACF v.rr.m SUBSYSTEM

**Explanation:** This message is for information only and indicates the current version v, release rr, and modification level m of the installed RACF product. Depending on the operands, one of the following groups of message lines may be displayed. “LU” in these messages is the abbreviation for “logical unit”.

When the APPL keyword is specified with no other keywords:

```
LU NAME  LU NAME  ...  LU NAME applname1
applname2 ... applname7
```

When the POE keyword is specified without the USER, GROUP, or SECLABEL keywords:

```
REMOTE LU NAME(S) ASSOCIATED WITH ACTIVE LOCAL LU NAME applname1 LU NAME apliname ... LU NAME poename1 poename2 ... poename7
```

When USER, GROUP, or SECLABEL keywords are specified:

```
LOCAL LU applname FOR REMOTE LU poename HAS THE FOLLOWING USER(S): USER = userid GROUP = group SECLABEL = seclabel
```

When the POE keyword is specified and there are no matches for a particular APPL:

```
NO REMOTE LU NAMES MATCHING poename WERE FOUND FOR LOCAL LU applname
```

When the user-group-seclabel combination cannot be located:

```
NO USERS MEET THE SPECIFIED CRITERIA
```

**System action:** The DISPLAY command continues processing any specified operands.

**Destination:** Descriptor codes are 5, 8, and 9. There are no routing codes for this message.

---

**IRR005I** DISPLAY COMMAND UNABLE TO LOCATE APPL APPL-name

**Explanation:** The APPL-name specified in the APPL keyword could not be found in the table of current local LU (logical unit) names. This message is produced for explicit APPL-name.

**System action:** The DISPLAY command stops without further processing.

**Operator response:** Check that the APPL-name name entered in the APPL keyword is correct. Reenter the command with the correct value. If the problem persists notify the system programmer or the security administrator.

**User response:** See the operator response.

**System programmer response:** If the APPL-name is known to exist in the table of current local LU-names, obtain diagnostic information such as a system dump containing the table of local LU names.

**Destination:** Descriptor code is 5. There are no routing codes for this message.

---

**IRR006I** DISPLAY COMMAND UNABLE TO LOCATE A MATCH FOR APPL APPL-name

**Explanation:** The APPL(APPL-name) specification was not matched by an entry in the table of local LU (logical unit) names. This message is produced when the APPL-name specification is of the form APPL(ABC*) or APPL(*).

**System action:** The DISPLAY command stops without processing.

**Operator response:** Check the APPL-name entered in the APPL keyword for correctness. Reenter the command with the correct value. If the problem persists notify the system programmer or the security administrator.

**User response:** See the Operator Response.

**System programmer response:** If the APPL-name is known to match at least one entry in the table of current local LU names, obtain diagnostic information such as a system dump containing the table of local LU names.

**Destination:** Descriptor code is 5. There are no routing codes for this message.

---

**IRR007I** DISPLAY COMMAND FOUND THAT THERE WERE NO LOCAL LUS CURRENTLY ACTIVE

**Explanation:** The DISPLAY command could not display any information because the table of local LU
(logical unit) names was empty.

**System action:** The DISPLAY command stops without further processing.

**Operator response:** No specific response is required for this message unless it is known that the table should not be empty. In that case, notify the system programmer or the security administrator.

**User response:** See the Operator Response.

**System programmer response:** If this message reflects a condition that should not be present, examine the console log to determine what operations have been performed on the table of local LU names.

**Destination:** Descriptor code is 5. There are no routing codes for this message.

---

**IRRD008I**  DISPLAY COMMAND UNABLE TO LOCATE USER INFORMATION FOR REMOTE LU NAME poename

**Explanation:** The DISPLAY command could not display any information because the list of signed-on users is empty.

**System action:** The DISPLAY command stops without further processing.

**Operator response:** No specific response is required for this message unless you know that the list should not be empty. In that case, if the list is empty, notify the system programmer or the security administrator.

**User response:** See the Operator Response.

**System programmer response:** If this message reflects a condition that should not be present, examine the console log to determine what operations have been performed on the list of signed-on users.

**Destination:** Descriptor code is 2. There are no routing codes for this message.

---

**IRRD009I**  DISPLAY COMMAND FOUND THAT THERE WERE NO USERS CURRENTLY SIGNED ON

**Explanation:** There are no users in the signed-on list or lists.

**System action:** The DISPLAY command stops without further processing.

**Operator response:** No response is required unless it is known that users are currently signed on. If users are signed on, verify that the DISPLAY command was correctly entered with the wanted keywords and associated operands. If the command was entered correctly and users should be signed on, reenter the command and if the condition persists, notify your system programmer.

**User response:** See the Operator Response.

**System programmer response:** Report this message along with the return code to your IBM Support Center.

---

**IRRD080I**  DISPLAY COMMAND FOUND AN ERROR. ABEND CODE IS abend_code-reason_code

**Explanation:** The DISPLAY command encountered an abnormal condition. The abend code and reason code describe the type of error that was encountered.

**System action:** The DISPLAY command stops processing.

**Operator response:** Notify the system programmer.

**User response:** Notify the system programmer.

**System programmer response:** Report this message ID and its contents to your IBM support center. For a description of the abend code and reason code, see Chapter 11, “RACF abend codes,” on page 393. If the abend code and reason code displayed in the message
RACDCERT command messages

IRRD101I  You are not authorized to issue the RACDCERT command.

Explanation:  One of the following conditions occurred:
  • You are not defined to RACF with sufficient authority to issue the RACDCERT command as specified.
  • RACF is not active.

System action:  RACDCERT command processing ends.

User response:  See your RACF security administrator.

IRRD102I  The user ID specified is not defined to RACF.

Explanation:  The user ID specified on the ID keyword of the RACDCERT command could not be found on the RACF database.

System action:  RACDCERT command processing ends.

User response:  Be sure the user ID is specified correctly and that the user is defined to RACF. Issue the command again.

IRRD103I  An error was encountered processing the specified input data set.

Explanation:  RACDCERT encountered an error related to the data set containing the digital certificate or certificate request.

System action:  RACDCERT command processing ends.

User response:  Check that the correct data set name was specified for the ADD, CHECKCERT, GENCERT, or MAP keywords. Check for additional error messages pertaining to the data set name.

Check that the data set attributes are variable blocked, not fixed blocked. You should then re-verify the record format of your data set with the digital certificate.

IRRD104I  The input data set does not contain a valid (certificate | certificate request).

Explanation:  RACDCERT encountered an error while attempting to analyze the digital certificate or certificate request contained in the data set.

System action:  RACDCERT command processing ends.

IRRD105I  No certificate information was found for user userid.

Explanation:  RACDCERT was unable to locate digital certificate information for the user ID indicated in the message.

System action:  RACDCERT command processing ends.

User response:  Check that the ID keyword was specified correctly.

IRRD106I  Additional information is required to identify the certificate.

Explanation:  RACDCERT located more than one digital certificate for this user. Sufficient information was not provided to uniquely identify the certificate to be acted on.

System action:  RACDCERT command processing ends.

User response:  Provide additional information about the DELETE or ALTER keyword to uniquely identify the digital certificate that you want deleted or altered. You might need one of the following to identify the certificate:
  • SERIALNUMBER and ISSUERSDN
  • LABEL

IRRD107I  No matching certificate was found for this user.

Explanation:  RACDCERT could not find a digital certificate for this user that matched the information provided.

System action:  RACDCERT command processing ends.

User response:  Check that the ID keyword was specified correctly. If you specified the SERIALNUMBER and ISSUERSDN keywords or the LABEL keyword, be sure that they were specified correctly. For ROLLOVER, also check the NEWLABEL keyword value. Issue the RACDCERT command with the LIST keyword to examine the user’s certificate information. The ISSUERSDN and LABEL must be specified in the same case as shown in the display, and
The certificate does not meet RACF requirements and cannot be used.

Explanation: The certificate being added may be valid, but, RACF cannot use it for one of the following reasons:

- The issuer’s distinguished name is too long. RACF is trying to use the hash algorithm used in the certificate signature to create a DGTCERT profile name that fits the maximum length of 246, but the hash algorithm is unknown to RACF.
- The combined length of the serial number and issuer’s distinguished name is too long to create a DGTCERT profile name. The combined length should not exceed the maximum length of 246 for a profile name.
- The certificate contains critical extensions that RACF does not recognize.
- The certificate version is greater than 3.
- The certificate contains nonstandard KeyUsage.

System action: RACDCERT command processing ends.

User response: The digital certificate found in the data set cannot be used by RACF. If you have more than one certificate, be sure that the correct one was placed in the data set. Otherwise, you must obtain a new certificate containing information that meets RACF requirements. If you cannot obtain another certificate, contact your system programmer.

System programmer response: Check that the certificate being used has been issued by the intended certifying authority. If necessary, report the problem to the IBM support center.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: This certificate already exists in the RACF database for a different user. The profile-name is truncated after 180 characters in order to fit within a single line of message output.

System action: RACDCERT command processing ends.

User response: Use RACDCERT CHECKCERT to determine if the digital certificate is defined for the correct user. A certificate can only exist for one user. You can perform one of the followings actions:

- To add the certificate to a different user perform the following steps:
  1. Use RACDCERT EXPORT to export the certificate and its private key, if any, to a data set.
  2. Use RACDCERT DELETE to delete the certificate.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: During command processing, RACDCERT issued a RACROUTE of the specified request type, and received a return code and reason code that were not expected.

System programmer response: Use the return code information in z/OS Security Server RACROUTE Macro Reference to determine the error condition and fix the error. If necessary, report the problem to the IBM support center.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: This certificate already exists in the RACF database for a different user. The profile-name is truncated after 180 characters in order to fit within a single line of message output.

System action: RACDCERT command processing ends.

User response: Choose a different label for the certificate and reissue the command.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: During command processing, RACDCERT issued a RACROUTE of the specified request type, and received a return code and reason code that were not expected.

System programmer response: Use the return code information in z/OS Security Server RACROUTE Macro Reference to determine the error condition and fix the error. If necessary, report the problem to the IBM support center.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: This certificate already exists in the RACF database for a different user. The profile-name is truncated after 180 characters in order to fit within a single line of message output.

System action: RACDCERT command processing ends.

User response: Choose a different label for the certificate and reissue the command.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: During command processing, RACDCERT issued a RACROUTE of the specified request type, and received a return code and reason code that were not expected.

System programmer response: Use the return code information in z/OS Security Server RACROUTE Macro Reference to determine the error condition and fix the error. If necessary, report the problem to the IBM support center.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: This certificate already exists in the RACF database for a different user. The profile-name is truncated after 180 characters in order to fit within a single line of message output.

System action: RACDCERT command processing ends.

User response: Choose a different label for the certificate and reissue the command.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: During command processing, RACDCERT issued a RACROUTE of the specified request type, and received a return code and reason code that were not expected.

System programmer response: Use the return code information in z/OS Security Server RACROUTE Macro Reference to determine the error condition and fix the error. If necessary, report the problem to the IBM support center.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: This certificate already exists in the RACF database for a different user. The profile-name is truncated after 180 characters in order to fit within a single line of message output.

System action: RACDCERT command processing ends.

User response: Choose a different label for the certificate and reissue the command.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: During command processing, RACDCERT issued a RACROUTE of the specified request type, and received a return code and reason code that were not expected.

System programmer response: Use the return code information in z/OS Security Server RACROUTE Macro Reference to determine the error condition and fix the error. If necessary, report the problem to the IBM support center.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: This certificate already exists in the RACF database for a different user. The profile-name is truncated after 180 characters in order to fit within a single line of message output.

System action: RACDCERT command processing ends.

User response: Choose a different label for the certificate and reissue the command.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: During command processing, RACDCERT issued a RACROUTE of the specified request type, and received a return code and reason code that were not expected.

System programmer response: Use the return code information in z/OS Security Server RACROUTE Macro Reference to determine the error condition and fix the error. If necessary, report the problem to the IBM support center.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: This certificate already exists in the RACF database for a different user. The profile-name is truncated after 180 characters in order to fit within a single line of message output.

System action: RACDCERT command processing ends.

User response: Choose a different label for the certificate and reissue the command.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: During command processing, RACDCERT issued a RACROUTE of the specified request type, and received a return code and reason code that were not expected.

System programmer response: Use the return code information in z/OS Security Server RACROUTE Macro Reference to determine the error condition and fix the error. If necessary, report the problem to the IBM support center.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: This certificate already exists in the RACF database for a different user. The profile-name is truncated after 180 characters in order to fit within a single line of message output.

System action: RACDCERT command processing ends.

User response: Choose a different label for the certificate and reissue the command.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: During command processing, RACDCERT issued a RACROUTE of the specified request type, and received a return code and reason code that were not expected.

System programmer response: Use the return code information in z/OS Security Server RACROUTE Macro Reference to determine the error condition and fix the error. If necessary, report the problem to the IBM support center.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: This certificate already exists in the RACF database for a different user. The profile-name is truncated after 180 characters in order to fit within a single line of message output.

System action: RACDCERT command processing ends.

User response: Choose a different label for the certificate and reissue the command.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: During command processing, RACDCERT issued a RACROUTE of the specified request type, and received a return code and reason code that were not expected.

System programmer response: Use the return code information in z/OS Security Server RACROUTE Macro Reference to determine the error condition and fix the error. If necessary, report the problem to the IBM support center.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: This certificate already exists in the RACF database for a different user. The profile-name is truncated after 180 characters in order to fit within a single line of message output.

System action: RACDCERT command processing ends.

User response: Choose a different label for the certificate and reissue the command.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: During command processing, RACDCERT issued a RACROUTE of the specified request type, and received a return code and reason code that were not expected.

System programmer response: Use the return code information in z/OS Security Server RACROUTE Macro Reference to determine the error condition and fix the error. If necessary, report the problem to the IBM support center.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: This certificate already exists in the RACF database for a different user. The profile-name is truncated after 180 characters in order to fit within a single line of message output.

System action: RACDCERT command processing ends.

User response: Choose a different label for the certificate and reissue the command.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: During command processing, RACDCERT issued a RACROUTE of the specified request type, and received a return code and reason code that were not expected.

System programmer response: Use the return code information in z/OS Security Server RACROUTE Macro Reference to determine the error condition and fix the error. If necessary, report the problem to the IBM support center.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: This certificate already exists in the RACF database for a different user. The profile-name is truncated after 180 characters in order to fit within a single line of message output.

System action: RACDCERT command processing ends.

User response: Choose a different label for the certificate and reissue the command.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: During command processing, RACDCERT issued a RACROUTE of the specified request type, and received a return code and reason code that were not expected.

System programmer response: Use the return code information in z/OS Security Server RACROUTE Macro Reference to determine the error condition and fix the error. If necessary, report the problem to the IBM support center.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: This certificate already exists in the RACF database for a different user. The profile-name is truncated after 180 characters in order to fit within a single line of message output.

System action: RACDCERT command processing ends.

User response: Choose a different label for the certificate and reissue the command.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: During command processing, RACDCERT issued a RACROUTE of the specified request type, and received a return code and reason code that were not expected.

System programmer response: Use the return code information in z/OS Security Server RACROUTE Macro Reference to determine the error condition and fix the error. If necessary, report the problem to the IBM support center.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: This certificate already exists in the RACF database for a different user. The profile-name is truncated after 180 characters in order to fit within a single line of message output.

System action: RACDCERT command processing ends.

User response: Choose a different label for the certificate and reissue the command.

The certificate cannot be added. Profile profile-name is already defined.

Explanation: During command processing, RACDCERT issued a RACROUTE of the specified request type, and received a return code and reason code that were not expected.
generating a new certificate using a certificate request, the certificate or certificate request has been altered and cannot be used. If you are adding or importing a non-self-signed certificate, either the certificate has been altered, or the CERTAUTH certificate that RACF is using to verify that the signature is not the correct CERTAUTH certificate. This means that the CERTAUTH certificate has a Subject Distinguished Name that matches the Issuer’s Distinguished Name in the input certificate but the key within the CERTAUTH certificate is not the one that was used to sign the input certificate. This can only happen if the given certificate authority is operating with multiple keys, which is typically a setup error. For example, it is possible that the RACDCERT GENCERT command was issued more than once specifying the same SUBJECTSDN.

**System action:** RACDCERT command processing ends.

**User response:** If the certificate or certificate request has been altered, obtain an unaltered copy and reissue the command. Ensure that there is no unexpected character set translation when the certificate or certificate request is transferred to the z/OS system. An unexpected translation might cause the signature to be invalid. If you are sure that the non-self-signed certificate you are adding or importing is valid, ensure that the correct CERTAUTH certificate is installed.

**Explanation:** You are using RACDCERT ADD, IMPORT, GENCERT, or REKEY to define a certificate to RACF. As a part of the definition process, RACF validates the date range on the certificate. This message might indicate that RACF has detected a potential date conflict. If error-description reads:

- "is self-signed", the certificate you are adding cannot be verified.
- "is expired", the last date for which the certificate is valid has passed.
- "has an incorrect date range", the date range of the certificate being added is not within the date range established by the CA (certificate authority) certificate.

**System action:** RACDCERT adds the certificate.

**User response:** Do one of the following tasks:

- If you want to alter the trust status of the certificate, issue the RACDCERT ALTER command.
- If the date range is incorrect, get either a new certificate or a new certificate authority certificate from the issuer and add the certificate or reissue the RACDCERT GENCERT or REKEY command specifying the correct date range.

**Explanation:** You are trying to add or generate a certificate from a certificate request. RACF cannot validate the signature because the algorithm that was used to generate the certificate’s signature or the

---

**IRRD113I • IRRD118I**

**IRRD113I** The certificate that you are [adding | creating] error-description. The certificate is added with [TRUST | NOTRUST | HIGHTRUST] status.

**Explanation:** You are using RACDCERT ADD, IMPORT, GENCERT, or REKEY to define a certificate to RACF. As a part of the definition process, RACF validates the date range on the certificate. This message might indicate that RACF has detected a potential date conflict. If error-description reads:

- "is self-signed", the certificate you are adding cannot be verified.
- "is expired", the last date for which the certificate is valid has passed.
- "has an incorrect date range", the date range of the certificate being added is not within the date range established by the CA (certificate authority) certificate.

**System action:** RACDCERT adds the certificate.

**User response:** Do one of the following tasks:

- If you want to alter the trust status of the certificate, issue the RACDCERT ALTER command.
- If the date range is incorrect, get either a new certificate or a new certificate authority certificate from the issuer and add the certificate or reissue the RACDCERT GENCERT or REKEY command specifying the correct date range.

**Explanation:** You are trying to add or generate a certificate from a certificate request. RACF cannot validate the signature because the algorithm that was used to generate the certificate’s signature or the
Certificate request's signature is not supported by RACF.

**System action:** If you are adding a certificate, the certificate is added with the trust status that you specified. If you did not specify a trust status, the certificate is added with NOTRUST status. If you are generating a certificate, the certificate is not created.

**User response:** Acquire a certificate or certificate request with a signature algorithm that is supported by RACF and reissue the RACDCERT ADD or RACDCERT GENCERT command. If the certificate was added, delete the old certificate.

---

**IRR119I** Certificate Authority not defined to RACF. Certificate added with [TRUST | NOTRUST | HIGHTRUST] status.

**Explanation:** You are adding or importing a certificate.
- If you are adding a self-signed certificate, the certificate content has not been verified.
- If you are adding a non-self-signed certificate, the certificate was signed by a certificate authority that you have not defined to RACF.

**System action:** The certificate is added with the trust status indicated by the message.
- If you are adding a self-signed certificate and you did not specify a trust status, the certificate is added with TRUST status.
- If you are adding a non-self-signed certificate and you did not specify a trust status, the certificate is added with NOTRUST status.
- The HIGHTRUST value will be used if specified, but will never be a default.

**User response:** Review the certificate status and change it if necessary. If you want to change the trust status, you should use the RACDCERT ALTER command.

---

**IRR120I** Incorrect use of [CERTAUTH | SITE]. A [Certificate Authority | Site Certificate] cannot own a key ring.

**Explanation:** You attempted to create a key ring for a site certificate or a certificate authority. This is not permitted. Only users may have key rings.

**System action:** The command fails.

**User response:** Correct the error and reissue the command.

---

**IRR121I** A ring name and label name must be specified.

**Explanation:** You issued a RACDCERT CONNECT or RACDCERT REMOVE command without a ring name or a label name specified. These commands require you to specify both a ring name and a label name.

---

**IRR122I** Ring ring-name cannot be added. It already exists.

**Explanation:** A ring may be added only once. Ring ring-name already exists. ring-name is truncated if its length plus the length of the static message text is more than is able to fit within a single line of output. This means that ring-name is truncated after approximately 200 characters.

**System action:** The command fails.

**User response:** Choose a different name for the ring and reissue the command.

---

**IRR123I** The certificate that you are processing is not encrypted. The certificate is not processed.

**Explanation:** You specified the PASSWORD keyword on a RACDCERT ADD or RACDCERT CHECKCERT request. The certificate contained in the data set you specified is not encrypted with a password.

**System action:** RACDCERT does not process the certificate.

**User response:** Check the data set to determine whether to use the PASSWORD keyword and reissue the command correctly.

---

**IRR124I** The certificate that you are processing cannot be decrypted with the specified PASSWORD. The certificate is not processed.

**Explanation:** The password you specified on a RACDCERT ADD or CHECKCERT request was not correct or the data set contains a certificate in a format that RACF cannot recognize. RACDCERT could not decrypt the certificate.

**System action:** RACDCERT does not process the certificate.

**User response:** Specify the correct password and reissue the command or acquire a certificate in a format that RACF can recognize.

---

**IRR125I** The key size that was specified or defaulted is not acceptable. The request is not processed.

**Explanation:** The RSA or DSA key size is not acceptable. The maximum key size is determined by United States export restrictions or internal system limits based on the key type. The minimum RSA or DSA key is 512 bits.
Generation of RACF non-ICSF RSA key certificates with a key size greater than 1024 requires that the CP Assist for Cryptographic Functions (CPACF) (feature code 3863) is enabled and the TDES function is available.

**System action:** RACDCERT does not process the request.

**User response:** Reissue the command with a smaller key size. For more information, see z/OS Security Server RACF Command Language Reference.

If you specified a non-ICSF RSA key size greater than 1024, ensure that the CP Assist for Cryptographic Functions (CPACF) (feature code 3863) is enabled and the TDES function is available.

**Explanation:** The certificate or certificate request extension contains information indicating that the certificate may not be used as a Certificate Authority certificate. The certificate is not added.

**System action:** The command terminates.

**Programmer response:** Acquire a correct certificate or certificate request and reissue the command.

The data set contains a PKCS12 encrypted certificate. The PASSWORD keyword must be specified to process the certificate. The certificate is not processed.

**Explanation:** The input data set is a PKCS #12 certificate package, which requires that you specify a password for RACDCERT to process the certificate. You must specify the password that is associated with the data set in the PASSWORD keyword.

**System action:** RACDCERT does not add the certificate.

**User response:** Issue the command with the PASSWORD keyword specified.

**Explanation:** The RACDCERT function function-name, which can be either GENCERT, GENREQ, or REKEY, requires a private key. GENCERT requires the private key that is associated with the certificate specified with the SIGNWITH keyword. GENREQ and REKEY require the private key that is associated with the certificate identified by the LABEL and the ID, SITE, or CERTAUTH keywords.

**System action:** RACDCERT does not process the request.
**User response:** Specify the required keyword and reissue the command.

**IRRD131I** The specified SUBJECTSDN exceeds the maximum allowed (nnn characters) by nnn characters. The request is not processed.

**Explanation:** The total length of the subject's distinguished name is limited to 229 characters for self-signed certificates and 255 characters for non-self-signed certificates.

**System action:** RACDCERT does not process the request.

**User response:** Reduce the total length of the distinguished name in the SUBJECTSDN keyword by at least nnn characters and reissue the command.

**IRRD132I** The certificate specified in the SIGNWITH keyword is not trusted. The certificate is added with NOTRUST status.

**Explanation:** You signed a certificate with a certificate that is marked as NOTRUST. Your certificate is added with NOTRUST status.

**System action:** RACDCERT adds the certificate with NOTRUST status.

**User response:** If you want to create a trusted certificate, either reissue the RACDCERT GENCERT command or issue the RACDCERT ALTER command to make your certificate trusted.

**IRRD133I** The NOTBEFORE value must be earlier than the NOTAFTER value. The certificate is not created.

**Explanation:** You attempted to create a certificate with a NOTBEFORE date that was later than the NOTAFTER date. This is not allowed.

**System action:** RACDCERT stops processing the request. The certificate is not created.

**User response:** Correct the NOTBEFORE and NOTAFTER dates and reissue the RACDCERT GENCERT command.

**IRRD134I** An error was encountered processing the specified output data set.

**Explanation:** RACDCERT encountered an error related to the data set containing the output of the RACDCERT command.

**System action:** RACDCERT command processing stops.

**User response:** Check to be sure that you entered the correct data set name. Check for additional errors pertaining to the data set name.

**IRRD135I** ICSF is not operational. The request is not processed.

**Explanation:** Either you are attempting to generate or add a certificate to the RACF database and have indicated that you want to use ICSF for key management, or you are attempting to generate a certificate or certificate request where the private key required to sign the information is a key stored in the PKDS. ICSF key management support is either unavailable, or the master key is absent or not set up correctly.

**System action:** The command is not processed.

**User response:** If ICSF key management is not required, reissue the command without requesting the key to be stored in the PKDS. If ICSF key management is required, report the error to your system programmer. Reissue the command after the problem has been corrected. For more information, see z/OS Security Server RACF Command Language Reference.

**System programmer response:** Ensure that ICSF is configured for PKA support and operational and that the master key of the PKDS is set up correctly. For more information, see z/OS Cryptographic Services ICSF System Programmer’s Guide.

**IRRD136I** MULTIID cannot be used for the function specified.

**Explanation:** You attempted a certificate related or key ring related function for the user ID MULTIID. This user ID is associated with filtering based on additional criteria, and can only be used for the mapping functions: MAP, ALTMAP, DELMAP, and LISTMAP.

**System action:** RACDCERT command processing ends.

**User response:** Correct the error and reissue the command.

**IRRD137I** Incorrect use of [CERTAUTH | SITE]. A [Certificate Authority | Site Certificate] cannot be used for a mapping function.

**Explanation:** You attempted to associate a mapping profile with the user ID associated with certificate authority certificates or site certificates. This is not permitted. Only users or MULTIID can be associated with a mapping profile.

**System action:** RACDCERT command processing ends.

**User response:** Correct the error and reissue the command.
IRRD138I The Label label-name is already in use.

Explanation: You attempted to associate a user ID with a mapping profile, and assign label-name to that association, or you attempted to change the label of an existing mapping profile to label-name. The label is already in use for the user specified in the RACDCERT command.

System action: RACDCERT command processing ends.

User response: Choose a different label and reissue the command.

IRRD139I This filter already exists. It cannot be added.

Explanation: You specified values for the IDNFILTER and SDNFILTER keywords that would create a filter that already exists in a mapping profile in the DIGTNMAP class. All filters must be unique.

System action: RACDCERT command processing ends.

User response: Choose a different filter value, or delete the existing mapping, and reissue the command.

IRRD140I The filter value does not begin with a valid prefix.

Explanation: You specified a value for the IDNFILTER or SDNFILTER keyword that does not begin with a valid prefix. The value must begin with an X.509 identifier such as C= or OU=.

System action: RACDCERT command processing ends.

User response: Specify a valid prefix for the filter value, and reissue the command.

IRRD141I The starting point specified for [IDNFILTER | SDNFILTER] results in a filter that is too long.

Explanation: You specified a value for the IDNFILTER or SDNFILTER keyword to be used as the starting point for a filter based on a certificate you have supplied in a data set. The resulting filter would exceed 255 characters from the specified starting point to the end of the actual name in the certificate.

System action: RACDCERT command processing ends.

User response: Use the CHECKCERT keyword to display the certificate, and reissue the command with a starting point value that is 255 characters or less from the end of the issuer's or subject's name.

IRRD142I No mapping profile with label label-name exists for this user ID.

Explanation: You specified a label name that does not exist for this user.

System action: RACDCERT command processing ends.

User response: Use the LISTMAP keyword without specifying a label to determine the label names that exist for this user. If you are attempting to alter or delete a mapping, reissue the RACDCERT command with the correct label.

IRRD143I No mapping profiles are associated with [user userid | MULTIID].

Explanation: You issued a RACDCERT LISTMAP command for a user who is not associated with any mapping profiles in the DIGTNMAP class.

System action: RACDCERT command processing ends.

User response: None.

IRRD144I A label is required to identify the mapping to be [altered | deleted].

Explanation: You specified ALTMAP or DELMAP without specifying a label. This user has more than one mapping profile entry associated with it, and a label is required to identify which mapping to change or delete.

System action: RACDCERT command processing ends.

User response: Reissue the RACDCERT command with the LABEL keyword specified.
IRRD146I  SDNFILTER cannot be specified with a partial issuer's name filter.

Explanation: You specified both SDNFILTER and IDNFILTER for the MAP function, with a certificate supplied in a data set. The value specified for IDNFILTER does not correspond to the beginning of the issuer's name in the certificate. This indicates that a partial issuer's name is to be used for the filter value. The SDNFILTER keyword cannot be used to specify a subject's name filter if IDNFILTER specifies a partial issuer's name.

System action: RACDCERT command processing ends.

User response: Reissue the RACDCERT command without the SDNFILTER keyword, or specify a value for the IDNFILTER keyword that will result in the full issuer's name being used in the filter.

IRRD147I  EXPORT in PKCS12 format requires a certificate with an associated non-ICSF private key. The request is not processed.

Explanation: A PKCS #12 certificate package contains a certificate and private key. The certificate you are trying to export either has no associated private key or has a private key stored in ICSF. (ICSF private keys are not exportable.)

System action: The command stops.

Programmer response: Do one of the following tasks:
1. Choose a certificate that has a non-ICSF private key.
2. Export in a CERT format that does not require a private key.

IRRD148I  EXPORT in PKCS12 format requires an encryption password. The PASSWORD keyword must be specified. The request is not processed.

Explanation: The data portion of a PKCS #12 certificate package is encrypted using a user specified password. The password was not specified.

System action: The command stops.

Programmer response: Reenter the command specifying the PASSWORD keyword.

IRRD149I  PKCS12 EXPORT package created with an incomplete certificate basing chain.

Explanation: RACF could not locate one of the signing certificates because either it is not installed as a CERTAUTH certificate or is expired. A PKCS #12 certificate package contains the end certificate being exported and any signing certificates needed to complete the basing chain (hierarchy) from end certificate to self-signed root certificate.

System action: An incomplete PKCS #12 certificate package is created.

Programmer response: If a complete PKCS #12 package is required, be sure that the appropriate non-expired signing certificates are installed under CERTAUTH. Reenter the command.

IRRD150I  Extra Certificate Authority Certificates ignored. Processing continues for the end-entity certificate only

Explanation: You are attempting to add either a PKCS #7 or PKCS #12 certificate package to RACF. The package contains an end-entity certificate and one or more Certificate Authority (CERTAUTH) certificates. You are not authorized to add CERTAUTH certificates.

System action: The command continues. However, the CERTAUTH certificates are not added.

User response: If the CERTAUTH certificates are required, see your RACF security administrator. The z/OS Security Server RACF Command Language Reference describes the authority required to issue the RACDCERT command.

IRRD151I  PKCS7 package created with an incomplete certificate basing chain

Explanation: You are attempting to export a PKCS #7 certificate package from RACF. A PKCS #7 certificate package contains the end-entity certificate being exported and any Certificate Authority (CERTAUTH) certificates needed to complete the basing chain (hierarchy) from end-entity certificate to self-signed root certificate. RACF could not locate one of the CERTAUTH certificates needed for one of the following reasons:
1. It is not installed as a CERTAUTH certificate.
2. It is expired.
3. You are not authorized to export CERTAUTH certificates.

System action: An incomplete PKCS #7 certificate package is created.

User response: If a complete PKCS #7 package is required, be sure that the appropriate non-expired Certificate Authority certificates are installed under CERTAUTH. Also, see your RACF security administrator. The z/OS Security Server RACF Command Language Reference describes the authority required to issue the RACDCERT command. Reenter the command.

IRRD152I  Root Certificate Authority not currently defined to RACF. Top CERTAUTH certificate added with the [TRUST | NOTRUST | HIGHTRUST] status

Explanation: You are attempting to add either a PKCS #7 or PKCS #12 certificate package to RACF. The
package contains an end-entity certificate and a chain of one or more Certificate Authority (CERTAUTH) certificates. The issuer of the top CA certificate (for example, the root Certificate Authority) is not currently defined to RACF. If the top CA certificate is a self-signed certificate, the certificate content has been verified using the public key contained in the certificate itself. If the top CA certificate is a non-self-signed certificate, the certificate was signed by a certificate authority that you have not defined to RACF, therefore, cannot be verified.

System action: The top CA certificate is added under CERTAUTH with the trust status displayed. See z/OS Security Server RACF Command Language Reference for information about how the trust status was determined. Processing continues for the remaining certificates in the package.

User response: Review the certificate status and change it if necessary. If you want to change the trust status, you should use the RACDCERT ALTER command.

IRRD153I • IRRD156I

Inconsistency detected for one or more Certificate Authority certificates. Processing continues for the end-entity certificate.

Explanation: You are attempting to add either a PKCS #7 or PKCS #12 certificate package to RACF. The package contains an end-entity certificate and one or more Certificate Authority (CERTAUTH) certificates. While adding the CERTAUTH certificates, an inconsistency was detected for one or more of these certificates. The inconsistency is one of the following tasks:
1. The certificate is expired.
2. The certificate has an incorrect date range relative to the issuing CA certificate. (The validity period is not completely contained within the validity period of the issuing CA certificate.)
3. The issuer of the certificate is missing from the certificate package and is not already installed under CERTAUTH.
4. The certificate has an unknown signature algorithm.

System action: The CERTAUTH certificates are added. In most cases, the trust status set for these certificates will be NOTRUST. See z/OS Security Server RACF Command Language Reference for information about how the trust status was determined. Processing continues for the end-entity certificate.

User response: If the CERTAUTH certificates are required, check the certificates that were added under CERTAUTH to determine which ones have the inconsistency. Contact your certificate supplier to determine if replacement certificates are available. If so, adding them will replace the inconsistent ones. Otherwise, if you want to use the certificates as is, you should change their status to TRUST. To change the trust status, you should use the RACDCERT ALTER command.

IRRD154I • PCICC is not operational. The request is not processed.

Explanation: You are attempting to add or generate a certificate and have indicated that you want to use the PCI cryptographic coprocessor (PCICC) or you are attempting to generate a certificate or certificate request where the private key required to sign the information is a PCICC key. The PCI cryptographic coprocessor is either not present or not operating.

System action: The command is not processed.

User response: If the PCI cryptographic coprocessor is not required, you can attempt to reissue the command without specifying the PCICC keyword. If the PCI cryptographic coprocessor is required, report the error to your system programmer. Reissue the command after the problem has been corrected. For more information, see z/OS Cryptographic Services ICSF System Programmer’s Guide.

IRRD155I • Source or target certificate ineligible for rollover. The rollover is not performed.

Explanation: You are attempting to roll over one certificate to another. At least one of the following conditions is true:
1. You specified the same certificate for both the source and the target.
2. The target certificate has already been the target of a previous rollover operation.
3. The target certificate has been used to sign other certificates.
4. The source or target certificate does not have a private key associated with it.

RACF will permit such a rollover only if the FORCE keyword is also specified.

System action: RACDCERT command processing ends.

User response: Use RACDCERT LIST to determine if the certificates you had specified are the ones you had intended to use. Reissue the command specifying the correct certificates, or FORCE keyword, if applicable.

IRRD156I • Keyusage is incompatible with Key algorithm.

Explanation: You are attempting to generate a certificate using either the RACDCERT TSO command or the R_PKIServ callable service. The KeyUsage value
is not compatible with the key algorithm.

If you are using the RACDCERT GENCERT command, the valid KeyUsages are:

- DSA
  - HANDSHAKE
  - DOCSIGN
  - CERTSIGN

If the keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, or decipherOnly bit is on in the request, you must specify compatible KeyUsage or key type values to override those contradicting values in the request.

- RSA
  - HANDSHAKE
  - DOCSIGN
  - CERTSIGN
  - KEYAGREE

- ECC
  - HANDSHAKE
  - DOCSIGN
  - CERTSIGN
  - KEYAGREE

If the keyEncipherment or dataEncipherment bit is on in the request, you must specify compatible KeyUsage or key type values to override those contradicting values in the request.

If you are using the R_PKIServ callable service GENCERT, REQCERT, or MODIFYREQS, the valid KeyUsages are:

- DSA
  - DIGITALSIGNATURE (DIGITALSIG)
  - NONREPUDIATION
  - KEYCERTSIGN
  - CRLSIGN

- RSA
  - DIGITALSIGNATURE (DIGITALSIG)
  - NONREPUDIATION
  - KEYCERTSIGN
  - CRLSIGN
  - KEYAGREE
  - DATAENCIPHERMENT (DATAENCIPH)

- ECC
  - DIGITALSIGNATURE (DIGITALSIG)
  - NONREPUDIATION

If the keyEncipherment or dataEncipherment bit is on in the request, you must specify compatible KeyUsage or key type values to override those contradicting values in the request.

- KEYCERTSIGN
- CRLSIGN
- KEYAGREE

If the keyEncipherment or dataEncipherment bit is on in the request, you must specify compatible keyusage or key type values to override those contradicting values in the request.

**System action:** RACDCERT or R_PKIServ processing ends. RACF prevents the request from completing.

**User response:** Select a different KeyUsage, generate a new PKCS #10 certificate, if applicable, or contact your system programmer or web page administrator.

**Application Programmer Response:** Modify the application invoking the R_PKIServ callable service to provide different KeyUsage values.

**Web Page Administrator Response:** If R_PKIServ is being invoked from the PKI Services CGIs, modify the certificate template definition in the pkiserv.tmpl file to provide different KeyUsage values in the <CONSTANT> section.

**Explanation:**
You are using RACDCERT ADD, RACDCERT REKEY, or RACDCERT GENCERT with an input request to define a certificate with a DSA key to RACF and you specified RSA, NISTECC, BPECC, PKDS, ICSF, or PCICC which is conflicting with the source certificate or certificate request.

**System action:** RACDCERT adds or generates the certificate with key type non-ICSF DSA.

**User response:** None.

**ICSF is not operational. ICSF private key not deleted.**

**Explanation:** While attempting to delete a certificate with a private key stored in ICSF, it was detected that ICSF was not operational.

**System action:** The request is processed, but the ICSF private key is not deleted.

**User response:** See the ICSF documentation to determine how to ensure that the ICSF service is operational and how the private key stored in ICSF can be deleted.

**System programmer response:** Ensure that ICSF is configured for PKA support and operational. For more information see z/OS Cryptographic Services ICSF System Programmer’s Guide.
IRR159I  The key size requires the use of a PCI Cryptographic Coprocessor. The PCICC keyword must be specified. The request is not processed.

Explanation: You are attempting to generate or add a certificate. The private key of the certificate is to be generated or saved as a software key. The requested private key size exceeds the limits set by the United States regulation and cannot be processed. However, RACF has detected the presence of a PCI cryptographic coprocessor (PCICC). The requested size can be acceptable if it is processed as a PCICC key.

System action: The command is not processed.

User response: If you are generating a certificate and a software key is required, reissue the command with a smaller key size. Otherwise, if a PCICC key is acceptable, reissue the command specifying PCICC. For more information, see z/OS Security Server RACF Command Language Reference.

IRR160I  WITHLABEL value cannot be used as a PKDS label.

Explanation: You are attempting to generate, add, or rekey a certificate and store its key in the ICSF PKDS. The WITHLABEL keyword was specified along with ICSF(*), PCICC(*), RSA(PKDS(*)) NISTECC(PKDS(*)), or BPECC(PKDS(*)), indicating that the WITHLABEL value should also be used for the PKDS label. The WITHLABEL does not meet the syntax requirements for a PKDS label. The allowed characters are alphanumeric, national (@,#,$) or period (.). Additionally, the first character must be alphabetic or national.

System action: The command is not processed.

User response: Reissue the command with a different PKDS label value. For more information, see z/OS Security Server RACF Command Language Reference.

IRR161I  The certificate cannot be (added | generated). The certificate's key is already stored under PKDS label 'pkds-label-value'.

Explanation: You are attempting to renew or readd a certificate and store its key in the ICSF PKDS. The certificate’s key has already been saved in the PKDS with the label displayed in the error message. The PKDS label may not be respecified.

System action: The command is not processed.

User response: Reissue the command without specifying a PKDS label value. For more information, see z/OS Security Server RACF Command Language Reference.

IRR163I  Insufficient authority to access token token-name

Explanation: You are attempting to perform an operation against the z/OS PKCS #11 token named token-name. ICSF determines that you do not have permission to perform the operation.

System action: RACDCERT command processing ends.

User response: Report the error to your RACF security administrator.

RACF Security Administrator Response: Determine if the user should have permission to perform the requested operation. If required, use PERMIT to add the user to the access list of the appropriate CRYPTOZ class profile. See z/OS Cryptographic Services ICSF Application Programmer's Guide for more information.

IRR165I  Cryptoz processing is not operational. The request is not processed.

Explanation: You are attempting to perform an operation on a z/OS PKCS #11 token. z/OS PKCS #11 processing is not active on the system.

System action: The command is not processed.

System programmer response: Ensure that ICSF is configured for z/OS PKCS #11 support and that ICSF is operational. For more information, see z/OS Cryptographic Services ICSF System Programmer’s Guide.

IRR166I  Token token-name does not exist.

Explanation: You are attempting to refer to a z/OS PKCS #11 token with the name token-name, which does not exist.

System action: RACDCERT command processing ends.

User response: Select a token name that exists and reissue the RACDCERT command.
User response: Choose a different name for the token and reissue the command.

**IRRD171I  Certificate has a key type not supported by Cryptoz. Bind not allowed.**

Explanation: You are attempting to bind a certificate to a z/OS PKCS #11 token. The certificate is found in RACF. However, the certificate has the following key type that is not supported by z/OS PKCS #11:

- The key algorithm of the certificate is RSA or ECC,
- but the associated private key is already stored in ICSF.

As a result, the certificate cannot be bound.

System action: The command fails.

User response: Use another certificate for the bind and reissue the command. If you must re-create the certificate, do not use the options to store the key in PKDS when generating the certificate.

**IRRD172I  Certificate with sequence number sequence-number in token token-name does not have a private key in RACF. The request is not processed.**

Explanation: You are attempting to unbind a certificate from a z/OS PKCS #11 token or delete the entire token. RACF has determined that the certificate mentioned in the message has an associated private key in the token. The certificate is defined to RACF, but without the associated private key. Completing the operation will permanently delete the private key. RACF permits the operation only if the FORCE keyword is also specified.

System action: The command fails.

User response: Use RACDCERT LISTTOKEN to determine if the token and certificate you specified are the ones that you want to use. Reissue the command specifying the correct token and certificate, or if applicable, the FORCE keyword.

**IRRD173I  Certificate with sequence number sequence-number in token token-name does not have a private key in RACF. The request is not processed.**
specifying the correct token and certificate, or if applicable, the FORCE keyword.

**IRRD174I** Token `token-name` contains object(s) that are not supported by RACF. The request is not processed.

**Explanation:** You are attempting to delete a z/OS PKCS #11 token. RACF has determined that the token contains objects that RACF cannot manage. Completing the operation will permanently delete these objects. RACF permits the operation only if the FORCE keyword is also specified.

**System action:** The command fails.

**User response:** Use RACDCERT LISTTOKEN to determine if the token you specified is the one you want to delete. Optionally use the z/OS ICSF PKCS11 token browser utility panels to see the contents of the objects that are not supported by RACF. Reissue the command specifying the correct token, or if applicable, the FORCE keyword.

**IRRD175I** The new profile for `class-name` will not be in effect until a SETROPTS REFRESH has been issued.

**Explanation:** The profile created in the specified class has been successfully added to the RACF database. However, the class specified is RACLISTed, so the change will not take effect until a SETROPTS command is issued to refresh the RACLISTed class.

**System action:** RACF updates the profile in the RACF database, but does not update the in-storage copy of the profile.

**User response:** None

**IRRD176I** RACLISTed profiles for `class-name` will not reflect the deletion(s) until a SETROPTS REFRESH is issued.

**Explanation:** The profile in the specified class has been successfully deleted from the RACF database. However, the class specified is RACLISTed, so the change will not take effect until a SETROPTS command is issued to refresh the RACLISTed class.

**System action:** RACF updates the profile in the RACF database, but does not update the in-storage copy of the profile.

**User response:** None

**IRRD177I** RACLISTed profiles for `class-name` will not reflect the update(s) until a SETROPTS REFRESH is issued.

**Explanation:** The profile in the specified class has been successfully updated in the RACF database. However, the class specified is RACLISTed, so the change will not take effect until a SETROPTS command is issued to refresh the RACLISTed class. However, if the update specified by the command does not actually change any value in the specified profile, the SETROPTS command is not necessary.

**System action:** RACF updates the profile in the RACF database, but does not update the in-storage copy of the profile.

**User response:** None

**IRRD178I** There was an error processing the DIGTRING profile `<profile-name>`. Processing has stopped.

**Explanation:** During command processing, RACDCERT LISTRING encountered an error when trying to retrieve the DIGTRING profile. The list of displayed DIGTRING profiles might be incomplete.

**System action:** RACDCERT command processing ends.

**User response:** Try to reissue the command. If the DIGTRING profile mentioned is defined with a generic character, turn off the generic characters for the DIGTRING class and reissue the command.

**IRRD179I** A token name and a label name must be specified.

**Explanation:** You are attempting to bind a RACF certificate to a z/OS PKCS #11 token, but you have not specified enough information. This command requires you to specify both a token name and a RACF certificate label name.

**System action:** The command fails.

**User response:** Correct the error and reissue the command. If you reissue the command specifying a label, you might also need to specify the owner ID(user-id | SITE | CERTAUTH).

**IRRD180I** A token name and a sequence number must be specified.

**Explanation:** You are attempting to import a z/OS PKCS #11 token certificate into RACF, but you have not specified enough information. This command requires you to specify both a token name and the sequence number of the certificate in the token.

**System action:** The command fails.

**User response:** Use RACDCERT LISTTOKEN to determine the correct token name and certificate sequence number. Correct the error and reissue the command.
Certificate with sequence number sequence-number in token token-name has a private key that cannot be imported. Certificate imported without the private key.

**Explanation:** You are attempting to import a certificate from a z/OS PKCS #11 token. RACF has determined that the certificate has an associated private key in the token. The private key cannot be imported for one of the following reasons:

- It is marked sensitive.
- It does not contain all the information required for RACF private keys.

**System action:** The command continues, but the private key is not imported.

**User response:** If you do not need a private key, do not take any remedial action. If you do need a certificate with a private key, choose another certificate to import. Use RACDCERT LISTTOKEN to determine if the token and the certificate you specified are the ones that you want to use. Reissue the command specifying the correct token and certificate.

**IRRD182I** Unexpected character encountered.

**Explanation:** The certificate or the certificate request specified in the RACDCERT command contains an unsupported character in the Subject Distinguished Name.

**System action:** RACDCERT command processing ends.

**User response:** Reissue the command with a request or certificate that contains supported characters only.

**IRRD183I** Certificate has a key size (size) not supported by ICSF for PKCS11 token. Bind incomplete.

**Explanation:** You are attempting to bind a certificate to a z/OS PKCS #11 token. The certificate is found in RACF. However, the certificate has a key size not supported by PKCS #11. As a result, the certificate is added to the token, but not the corresponding public key or private key.

**System action:** RACDCERT BIND processing ends after the certificate is added to the token.

**User response:** You may issue the RACDCERT UNBIND command to remove the certificate. Then use another certificate with the supported key size for the bind and reissue the BIND command.

**IRRD184I** The key size exceeds the limit of ICSF.

**Explanation:** You are attempting to generate or add a certificate. The private key of the certificate is to be generated or saved as a hardware key. The requested private key size exceeds the limits supported by the ICSF and cannot be processed. However, RACF has detected that the system has no export restriction. The requested size can be acceptable if it is processed as a software key.

**System action:** RACDCERT does not process the request.

**User response:** If you are generating a certificate and a hardware key is required, reissue the command with a smaller key size. Otherwise, if a software key is acceptable, reissue the command without specifying any key type.

**IRRD185I** The key size that was specified for an Elliptic Curve Cryptography (ECC) key is not acceptable.

**Explanation:** The specified key size is not valid. If you specify NISTECC, the acceptable key sizes are 192, 224, 256, 384, and 521. If you specify BPECC, the acceptable key sizes are 160, 192, 224, 256, 320, 384, and 512.

**System action:** RACDCERT does not process the request.

**User response:** Reissue the command specifying a valid key size. See z/OS Security Server RACF Command Language Reference for more information.

**IRRD186I** A Diffie-Hellman certificate can not be used to sign other certificates.

**Explanation:** An Elliptic Curve Cryptography (ECC) certificate with only the keyAgreement keyusage set (or together with encipherOnly or decipherOnly) is an ECC Diffie-Hellman certificate. The intended usage is for key exchange, not for signing. Any RACDCERT commands that involve signing with this type of certificate fails. For example, GENREQ or REKEY on an ECC Diffie-Hellman certificate or GENCERT a self-signed or GENCERT SIGNWITH an ECC Diffie-Hellman certificate.

**System action:** RACDCERT does not process the request.

**User response:** Reissue the command using a certificate that is not an ECC Diffie-Hellman certificate, or reissue the command specifying other KeyUsage bits in addition to KEYAGREE.
RACDCERT REKEY, or RACDCERT GENCERT with an input request to define a certificate with an RSA key to RACF and you specified NISTECC, BPECC, or DSA which is conflicting with the source certificate or certificate request.

**System action:** RACDCERT adds or generates the certificate with the original key type RSA.

**User response:** None.

---

The certificate is [added | generated] with key type [NISTECC | BPECC]. The specified keyword [ICSF | PCICC | RSA | DSA | NISTECC | BPECC] is ignored.

**Explanation:** You are using RACDCERT ADD, RACDCERT REKEY to define a certificate with an ECC key to RACF and you specified DSA, RSA, ICSF, or PCICC which is conflicting with the source certificate, or you are using RACDCERT GENCERT with an input request containing a NISTECC key and you specified BPECC, or you are using RACDCERT GENCERT with an input request containing a BPECC key and you specified NISTECC.

**System action:** RACDCERT adds or generates the certificate with the original key type NISTECC or BPECC.

**User response:** None.

---

The key type or the key size that was defaulted for an Elliptic Curve Cryptography (ECC) key causes a conflict.

**Explanation:** You specified RACDCERT REKEY to renew an ECC certificate but specified only a key type or only a key size. Either the default key type does not match the specified key size, or the default key size does not match the specified key type. The valid key sizes for NISTECC certificate are 192, 224, 256, 384, and 521. The valid key sizes for BPECC certificate are 160, 192, 224, 256, 320, 384, and 512.

**System action:** RACDCERT does not process the request.

**User response:** Reissue the command specifying an appropriate key size or key type. See [z/OS Security Server RACF Command Language Reference](https://www.ibm.com/support/knowledgecenter/p5831_13.1.0/com.ibm.zos.rscc.security/raccln2.html) for more information.

---

Insufficient authorization to ICSF service name.

**Explanation:** The RACDCERT request could not be performed because there is insufficient authorization to the ICSF service identified by name.

**System action:** RACDCERT command processing ends.

---

Insufficient authorization to ICSF key label.

**Explanation:** The RACDCERT request could not be performed because there is insufficient authorization to the PKDS label name specified by the issuer.

**System action:** RACDCERT command processing ends.

---

The specified key label does not exist.

**Explanation:** The RACDCERT request could not be performed because the specified label for the required public key in the ICSF PKDS does not exist.

**System action:** RACDCERT command processing ends.

**User response:** Reissue the command specifying a valid key label.

---

You cannot specify a request data set with the FROMICSF keyword. The certificate was not created.

**Explanation:** The RACDCERT GENCERT command was issued using an existing public key from the ICSF PKDS to define a certificate. A certificate cannot be defined if the RACDCERT GENCERT command is issued when a request data set is specified.

**System action:** RACDCERT command processing ends.

**User response:** Reissue the command without specifying a request data set.

---

The key type that corresponds to this PKDS label is not supported.

**Explanation:** The RACDCERT GENCERT command was issued using an existing public key from the ICSF PKDS to define a certificate. However, the key type is not supported when using FROMICSF.
**User response:** Reissue the command specifying a valid key label.

**Explanation:**

The certificate cannot be generated. The PKDS label is already associated with the certificate contained in the profile identified in message IRRD196I.

**System action:** RACDCERT command processing ends.

**User response:** Reissue the command specifying a valid key label.

**Explanation:**

This message is used to display a DIGTCERT class profile name containing a digital certificate. The message that precedes this one provides the context under which the profile name is displayed.

**System action:** See the message that precedes this one.

**User response:** See the message that precedes this one.

**Explanation:**

The certificate has a key type not supported by RACF. IMPORT failed.

**System action:** RACDCERT does not process the request.

**User response:** Reissue the command specifying a valid key size or key type. See z/OS Security Server RACF Command Language Reference for more information.
SIGNOFF command messages

IRRE001I | SIGNOFF ENCOUNTERED AN ERROR WHILE USING TSO PARSE, PARSE RETURN CODE WAS \(nn\)
---|---
**Explanation:** During the parse of the SIGNOFF command image, the TSO parse facility returned return code \(nn\), which is documented in \[z/OS TSO/E Programming Services\] in the section discussing IKJPARS.

**System action:** The SIGNOFF command stops processing and does not display any of the requested information.

**Operator response:** Verify that the SIGNOFF command entered was correctly entered with the wanted keywords and associated operands. Reenter the command. If the condition persists, notify your system programmer.

**User response:** See the Operator Response.

**System programmer response:** Examine the original SIGNOFF command image for possible specification errors. Use the \(nn\) value to determine the specific cause of the TSO Parse condition.

**Destination:** Descriptor code is 5. There are no routing codes for this message.

IRRE001I | UNIDENTIFIED TEXT OR KEYWORD \(text\) IN SIGNOFF COMMAND.
---|---
**Explanation:** The \(text\) character string was present in the SIGNOFF command image and was not recognized as a valid keyword.

**System action:** The SIGNOFF command stops.

**Operator response:** Examine the SIGNOFF command image and correct the text indicated by the \(text\) string. For information about the SIGNOFF command, see \[z/OS Security Server RACF Command Language Reference\]

**User response:** See the Operator Response.

**System programmer response:** See the Operator Response.

**Destination:** Descriptor code is 1. Routing codes are 2 and 9.

IRRE001I | SYSTEM AUTHORIZATION FACILITY REQUEST ENDED WITH A RETURN CODE OF \(code\)
---|---
**Explanation:** The attempt to issue a SIGNOFF request ended with a return code of \(code\). This \(code\) has been returned by the System Authorization Facility (SAF) router. For an explanation of the return code, see \[z/OS Security Server RACROUTE Macro Reference\]

**System action:** The SIGNOFF command stops without further processing. Message IRRE006I follows this message with information about the return and reason codes from the RACF SIGNOFF request.

**Operator response:** Notify either the system programmer or the security administrator. Note whether the SIGNOFF command provided any previous messages and whether a system dump was taken.

**User response:** See the Operator Response.

**System programmer response:** Determine what keywords and operands are contained in the SIGNOFF command. Examine the portion of console log recorded near the time of this message for the presence of other messages that might provide further information. Also, examine the system dump data sets for the presence of a dump resulting from this condition.

**Destination:** Descriptor code is 1. Routing codes are 2 and 9.
examine the system dump data sets for the presence of a dump resulting from this condition. Message IRRE006I follows this message with information about the return and reason codes from the RACF SIGNOFF request.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRE005I THE RACF SIGNOFF REQUEST WAS UNABLE TO LOCATE USER = userid
GROUP = group

Explanation: The user ID-group combination could not be located by the RACF SIGNOFF process.

System action: The SIGNOFF command continues with requests for other APPL values if specified.

Operator response: Verify that the SIGNOFF command was correctly entered with the wanted keywords and associated operands. If the command was entered correctly and userid should be present, reenter the command and if the condition persists, notify your system programmer.

User response: See the "Operator Response".

System programmer response: Examine the original SIGNOFF command image for possible specification errors. Examine the console logs to determine whether the specified user ID was previously signed off or some other type of abnormal condition occurred.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRE006I RACROUTE TYPE=SIGNOFF REQUEST ENDED WITH A RETURN
CODE OF return-code, REASON CODE OF reason-code

Explanation: This message can occur for either of the following conditions:

• The System Authorization Facility (SAF) returned a code of zero, but the RACF SIGNOFF request received an unexpected return code.

• The System Authorization Facility (SAF) received a nonzero return code that was previously shown in message IRRE004I.

System action: The SIGNOFF command stops without further processing.

Operator response: Notify either the system programmer or the security administrator. Note whether the SIGNOFF command has provided any previous messages and whether a system dump has been taken.

User response: See the Operator Response.

System programmer response: Determine what keywords and operands are contained in the SIGNOFF command. Examine the portion of the console log recorded before this message for the presence of other messages that might provide further information. Also, examine the system dump data sets for the presence of a dump resulting from this condition. See Server RACROUTE Macro Reference for an explanation of the return code and reason code.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRE007I SIGNOFF COMMAND REQUIRES THE
keyword KEYWORD TO BE SPECIFIED

Explanation: The SIGNOFF command requires that the APPL, POE, and USER keywords be specified.

System action: The SIGNOFF command stops without further processing.

Operator response: Reenter the command with the correct keywords.

User response: See the Operator Response.

System programmer response: See the Operator Response.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRE008I SIGNOFF COMMAND DOES NOT ALLOW PARTIAL GENERICS FOR
THE keyword KEYWORD

Explanation: Partial generics (A*) were specified for the keyword, which only allows for full generics or non-generics.

System action: The SIGNOFF command stops.

Operator response: Reenter the command specifying a fully qualified operand for keyword.

User response: See the Operator Response.

System programmer response: None.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRE009I SIGNOFF COMMAND COMPLETED

Explanation: This message is produced when the SIGNOFF command has completed its processing without error.

System action: The SIGNOFF command continues to normal termination.

Destination: Descriptor code is 5. There are no routing codes for this message.
IRRE010I  SIGNOFF COMMAND UNABLE TO LOCATE APPL APPL-name

Explanation: The APPL-name specified in the APPL keyword could not be found in the table of current local LU (logical unit) names. This message is produced for explicit APPL-name.

System action: The SIGNOFF command stops without further processing.

Operator response: Check the APPL-name entered in the APPL keyword for being correct. Reenter the command with the correct value. If the problem persists notify the system programmer or the security administrator.

User response: See the Operator Response.

System programmer response: If the APPL-name is known to exist in the table of current local LU names, obtain diagnostic information such as a system dump containing the table of local LU names.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRE011I  SIGNOFF COMMAND UNABLE TO LOCATE A MATCH FOR APPL APPL-name

Explanation: The APPL(APPL-name) specification was unable to find a match in the table of local LU (logical unit) names. This message is only produced when the APPL-name specification is of the form APPL(ABC*) or APPL(*).

System action: The SIGNOFF command stops without further processing.

Operator response: Check the APPL-name entered in the APPL keyword for being correct. Reenter the command with the correct value. If the problem persists notify the system programmer or the security administrator.

User response: See the operator response.

System programmer response: If the APPL-name is known to match at least one entry in the table of current local LU-names, then obtain diagnostic information such as a system dump containing the table of local LU names.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRE012I  SIGNOFF COMMAND FOUND THAT THERE WERE NO APPLS CURRENTLY SIGNED ON

Explanation: The SIGNOFF command could not successfully execute because the list of local LU (logical unit) names does not exist.

System action: The SIGNOFF command stops without further processing.

Operator response: No specific response is required for this message unless it is known that the list should not be empty. In that case, notify the system programmer or the security administrator.

User response: See the Operator Response.

System programmer response: If this message reflects a condition that should not be present, examine the console log to determine what operations have been performed on the list of local LU names.

Destination: Descriptor code is 5. There are no routing codes for this message.

IRRE080I  SIGNOFF COMMAND ENCOUNTERED AN ERROR. ABEND CODE IS abend_code-reason_code.

Explanation: During the normal processing of the SIGNOFF request, an abnormal condition was detected. The abend_code and reason_code are displayed. Display the system dump data sets for an accompanying diagnostic dump.

System action: The SIGNOFF command stops processing.

Operator response: Notify the system programmer.

User response: Notify the system programmer.

System programmer response: Report this message ID and its contents to your IBM support center. For a description of the abend code and reason code, see Chapter 11, “RACF abend codes,” on page 393. If the abend code and reason code displayed in the message do not appear in this information, see the system codes information for the MVS system at your installation.
RRSF send request handling task messages

**IRRF010I**  RACF WAS UNABLE TO LOAD COMMUNICATION ROUTINE (load module). REMOTE RACF PROCESSING USING APPC IS DEACTIVATED.

Explanation: The RACF subsystem address space issued the MVS macro LOAD to bring the load module into the RACF subsystem address space. This load module is needed to do any of the following tasks:
- Issue the appropriate APPC/MVS verb
- Build a connection with another node
- Send to and receive data from a remote node
- Process requests for the local node

System action: No attempt is made to register as an APPC/MVS server or to activate connections to other nodes. The local node processing is not activated. Any TARGET command requests to change the state of the connection to other nodes are ignored. The RACF subsystem address space saves the request that was issued. After the connection is made, RACF sends the request to the indicated node.

Operator response: Determine why the requested load module could not be found and loaded into the RACF subsystem address space. When the problem has been corrected, issue the RESTART CONNECTION command. This causes the RACF subsystem address space to attempt to bring the needed load modules into the RACF subsystem address space.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

**IRRF081I**  subsystem-name SUBSYSTEM SEND REQUEST HANDLING TASK ENCOUNTERED AN ERROR. ABEND CODE IS abend-code. SEND REQUEST TASK ENDING.

Explanation: The SEND request task was routing a work request to its destination on another node. This message appears when an abnormal event occurs.

System action: The SEND handler releases system resources it holds and ends processing.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of ABEND, the subtask should resume processing any work in its input queue. See “Actions to Recover from an RRSF Failure” in z/OS Security Server RACF Diagnosis Guide for a complete discussion.

Operator response: Report the occurrence of the message to the system programmer.

Problem Determination: See z/OS MVS System Codes for an explanation of these codes. The task that started the SEND request task attempts to restart the task. Verify that message IRRB020I was issued showing that the task restart was successful.

Destination: Descriptor code is 6. Routing code is 2.
RRSF PARMLIB and initialization messages

IRRG001I subsystem-name SUBSYSTEM UNABLE TO OPEN MEMBER IRROPTyy IN THE RACF PARAMETER LIBRARY.

Explanation: OPEN processing failed on the indicated subsystem for member IRROPTyy of the RACF parameter library. No configuration statements from this member of the RACF parameter library will be processed.

System action: None.

Operator response: Report the text of this message to the system programmer.

System programmer response: If the RACF parameter library member appears to be valid, report the occurrence of the error to the IBM support center.

Destination: Descriptor code is 6. Routing code is 2.

IRRG002I subsystem-name SUBSYSTEM COULD NOT LOCATE THE RACFPARM DD STATEMENT FOR THE RACF PARAMETER LIBRARY DATA SET.

Explanation: This message is displayed for one of the following reasons:

- You specified PARM='OPT=xx' on the EXEC JCL statement in the RACF procedure in SYS1.PROCLIB. However, you did not also supply the RACFPARM DD statement to identify the RACF parameter library data set containing the IRROPTxx member.
- You issued a SET INCLUDE(xx) command when the RACFPARM DD statement does not exist.

Because RACF cannot locate this data set, the commands contained within the IRROPTxx member are not processed. Therefore, if this message was displayed during RACF subsystem address space initialization, the RACF remote sharing facility is not activated.

System action: If this message was displayed during RACF subsystem address space initialization, initialization continues without activating RRSF. Any updates you make to the RACF database are not propagated to any other RACF database in your RRSF configuration until the problem is resolved. If the message was issued as a result of a SET INCLUDE(xx) command entered as an operator command, the command ends.

Operator response: Contact your system programmer.

System programmer response: The started procedure for the RACF subsystem in SYS1.PROCLIB must be updated to provide the RACFPARM DD statement, which identifies the data set that contains the IRROPTxx member. For information about how to update your started procedure for remote sharing, see z/OS Security Server RACF System Programmer’s Guide.

Destination: Descriptor code is 6. Routing code is 2.

IRRG006I A COMMAND IN PARAMETER LIBRARY MEMBER IRROPTyy HAS EXCEEDED THE MAXIMUM OF number CONTINUATION LINES.

Explanation: Commands to be processed from the RACF parameter library must not exceed number continuation lines. A parameter library command that exceeds this limit was detected and was not processed.

System action: None.

Operator response: See accompanying message IRRG007I for an indication of which command was in error.

Destination: Descriptor code is 6. Routing code is 2.
**Explanation:** xxxxxxxxxxxxxxxxxx is the first portion of the command that was ignored because of its excessive length. See preceding message IRRG006I.

**System action:** None.

**Operator response:** Report the text of this message to the system programmer.

**System programmer response:** Shorten the command, or remove it from the RACF parameter library.

**Destination:** Descriptor code is 6. Routing code is 2.

**Explanation:**

- This message indicates that processing of the IRROPTyy member of the RACF parameter library was begun by the indicated subsystem.

**System action:** Configuration statements (commands) within the RACF parameter library member are read and processed.

**Operator response:** None.

**Destination:** Descriptor code is 6. Routing code is 2.

**Explanation:** One or more recursive references to RACF parameter library member IRROPTyy have been detected during parameter library processing by the indicated subsystem. The recursive references are not processed. However, other RACF parameter library processing continues.

**System action:** None.

**Operator response:** Report the text of this message to the system programmer.

**System programmer response:** Remove all recursive references from the RACF parameter library.

**Destination:** Descriptor code is 6. Routing code is 2.

**Explanation:** This message indicates that processing of the IRROPTyy member of the RACF parameter library was completed by the indicated subsystem.

**System action:** None.

**Operator response:** None.

**Destination:** Descriptor code is 2. Routing code is 1.

**Explanation:** The active IFAPRDxx members of the SYSLPARMLIB contain a PRODUCT entry that enables the RACF (5695-039) but not the z/OS Security Server feature. Starting with OS/390 Release 3, the RACF function was shipped only as a part of the OS/390 Security Server feature. The RACF function can be used only when it is ordered and enabled as the z/OS Security Server feature.

**System action:** The RACF component of the z/OS Security Server initializes to provide you with a system you can use to correct the IFAPRDxx entries for RACF and the z/OS Security Server feature. During initialization, RACF registers as the z/OS Security Server, not as the RACF product.

**System programmer response:** Correct the IFAPRDxx entries according to your licensing agreements and IPL the system.

- If the z/OS Security Server feature has already been ordered, change the Security Server feature’s STATE value to ENABLED in the appropriate IFAPRDxx member.

- If the RACF function is required but the OS/390 Security Server feature was not ordered, order the feature from IBM and change its STATE value to ENABLED.

- If the RACF or DCE Security Server functions are required, do one of the following tasks:
  - Remove the RACF (5695-039) entry from the appropriate IFAPRDxx member
  - Change its STATE value to DISABLED

  For additional information, see [z/OS MVS Product Management](https://www.ibm.com).
IRRG080I  subsystem-name SUBSYSTEM PARAMETER LIBRARY HANDLING ENCOUNTERED AN ERROR. ABEND CODE IS returncode-reasoncode.

Explanation: RACF parameter library processing ended abnormally for the indicated subsystem, with the given return and reason codes. This message is written to the SYSLOG.

Operator response: Report the occurrence of the message to the system programmer.

System programmer response: Gather appropriate diagnostic information and contact the IBM support center.

SET command messages

IRRH001I  subsystem-name SUBSYSTEM SET COMMAND ENDED IN RECURSIVE ABEND.

Explanation: The SET command abnormally ended in its attempt to recover from a prior abend on the indicated subsystem.

System action: None.

Operator response: Report the occurrence of the message to the system programmer.

System programmer response: Gather appropriate diagnostic information and contact the IBM support center.

Destination: Descriptor code is 6.

IRRH002I  subsystem-name SUBSYSTEM SET COMMAND ENDED IN ERROR.

Explanation: The SET command encountered an error during processing on the indicated subsystem. See any accompanying messages for more specific error information.

System action: None.

Operator response: Report the occurrence of the message to the system programmer.

System programmer response: Gather appropriate diagnostic information and contact the IBM support center if the accompanying error messages do not indicate user error.

Destination: Descriptor code is 6.

IRRH003I  subsystem-name SUBSYSTEM SET COMMAND HAS COMPLETED SUCCESSFULLY.

Explanation: The SET command was processed by the subsystem-name subsystem without any errors.

System action: None.

Operator response: None.

Destination: Descriptor code is 6.

IRRH004I  subsystem-name SUBSYSTEM INFORMATION:

Explanation: This message precedes the remainder of the output displayed by SET LIST processing.

Operator response: None.

Destination: Descriptor code is 6.

IRRH005I  subsystem-name SUBSYSTEM INFORMATION:

Explanation: This message precedes the remainder of the output displayed by SET LIST processing.

Operator response: None.

Destination: Descriptor code is 6.

IRRH006I  MORE THAN FOUR USERS WERE SPECIFIED WITH THE OUTPUT AND NOTIFY KEYWORDS ON THE SET COMMAND.

Explanation: On the SET command, more than four users were specified with the OUTPUT and NOTIFY keywords. The combination of users specified on the two keywords can be a maximum of four different users. In other words, the cumulative total of unique users may not exceed four in both the OUTPUT and NOTIFY keywords. The same four users may be specified on each keyword. However, if four users are specified on one of the keywords, a (different) fifth user may not be specified on the other keyword. For example, if four users are specified on the OUTPUT keyword, a fifth user may not be specified on the NOTIFY keyword.

System action: Command processing fails to complete.

User response: Issue the command again, specifying no more than four different users with the OUTPUT and NOTIFY keywords.

Destination: Descriptor code is 6.
IRRH007I operand SPECIFIED ON THE | ALWAYS | WARN | FAIL | KEYWORD OF THE SET COMMAND IS NOT VALID.

Explanation: On the indicated SET command keyword, an operand was specified with incorrect syntax. The correct syntax is any of the following:

- node.userid
- .userid
- &RACUID

System action: Command processing fails to complete.

User response: Issue the command again, correcting the operand that is in error.

Destination: Descriptor code is 6.

IRRH080I subsystem-name SUBSYSTEM SET COMMAND ENCOUNTERED AN ERROR. ABEND CODE IS returncode-reasoncode.

Explanation: The SET command processed by the subsystem-name subsystem ended abnormally, with the given return and reason codes.

Operator response: Report the occurrence of the message to the system programmer.

System programmer response: Gather appropriate diagnostic information and contact the IBM support center.

Destination: Descriptor code is 6.

IRRH082I THE TRACE KEYWORD REQUIRES ADDITIONAL SPECIFICATION.

Explanation: The TRACE keyword requires the specification of 1 or more of its options.

System action: The SET command ends in error.

Operator response: Reissue a corrected version of the command, if necessary. See z/OS Security Server RACF Command Language Reference for the syntax of the SET command.

Destination: Descriptor code is 6.

IRRH083I THE GENERICANCHOR KEYWORD REQUIRES ADDITIONAL SPECIFICATION.

Explanation: The GENERICANCHOR keyword requires the specification of SYSTEM or JOBNAME and COUNT or RESET keywords.

System action: Command processing ends.

Operator response: Reissue the command with the additional required keywords. See z/OS Security Server RACF Command Language Reference for the syntax of the SET command.

Destination: Descriptor code is 6.

IRRH084I THE SET COMMAND HAD NO EFFECT ON THE GENERICANCHOR SETTINGS.

Explanation: The SET command was issued with the GENERICANCHOR keyword and the JOBNAME subkeyword. You specified a jobname or jobnames, which is not in the list of jobnames that contain specific generic anchor settings.

System action: No changes are made to the generic anchor values.

User response: Verify that the jobnames specified on the SET GENERICANCHOR command are the intended jobnames.
IRRI000I  •  IRRI005I

Destination:  Descriptor code is 6.

**RRSF handshaking messages**

**IRRI000I**  LOCAL RACF NODE local-node  
[SYSNAME system-name] IS  
ATTEMPTING TO CONTACT  
PARTNER RACF NODE partner-node  
[SYSNAME system-name].

Explanation:  This is an informational message only. One or more RACF TARGET commands were issued at the local RACF node local-node that caused it to attempt to establish communications with the partner node partner-node. The local node waits for a response from the partner (the partner should issue its own TARGET command). Once the partner has responded, information is exchanged and an attempt is made to open up RACF communication between these two nodes. This is known as entering the OPERATIVE ACTIVE state. This message is written to the SYSLGLOG when SYSNAME information is present for one or both of the nodes in this message, the node that precedes the SYSNAME is a multisystem node.

System programmer response:  If you receive this message and do not get a response either confirming or denying communication, ensure that the partner RACF node did issue a TARGET statement for this node (with the correct LU name, if APPC is being used, or the correct host address, if TCP is being used). A TARGET NODE (node-name) LIST command can be issued on the partner node to list the node definition as it is defined here. You should also check for communication protocol failures (that is, APPC or TCP), because that is the means RACF is using to communicate with the partner.

**IRRI000I**  RACF COMMUNICATION WITH  
NODE partner-node [SYSNAME system-name] HAS BEEN SUCCESSFULLY ESTABLISHED.

Explanation:  This is an informational message only. One or more RACF TARGET commands were issued that caused RACF to establish this communication link with the partner node. RACF on each node has successfully exchanged information and both have agreed to allow the communication. Communication is now considered OPERATIVE ACTIVE between these two nodes. If SYSNAME information is present in this message, the partner node partner-node is a multisystem node.

System programmer response:  No response is needed if you expected RACF to be communicating with RACF on the partner node. Otherwise, you might want to issue RACF TARGET commands to remove the communication path or modify the RACF parameter library commands that you currently run during RACF subsystem initialization.

**IRRI004I**  ATTENTION: LOCAL NODE local-node  
[SYSNAME system-name] HAS  
TEMPLATE VERSION xxxxxx.  
PARTNER NODE partner-node  
[SYSNAME system-name] HAS  
TEMPLATE VERSION xxxxxx.

Explanation:  This is an attention message only. You can choose whether to act immediately. RACF checks certain data between the partner node and the local node to determine whether a command could run on one node but not the other. The template level is an example of this data and a mismatch has been detected. Adding a field on one node may work, but fail on the other node until the corresponding template update takes place on that node. If SYSNAME information is present for one or both of the nodes in this message, the node that precedes the SYSNAME is a multisystem node.

System action:  If no error messages are issued with this attention message, RACF still attempts to move this node pair into the OPERATIVE ACTIVE state. Message IRRI001I tells you when the OPERATIVE ACTIVE state is reached.

System programmer response:  Evaluate the template levels in the message. If you do not plan to add or alter a profile specifically using the fields in the more recent version of the templates, you may ignore this message until the next service upgrade causes the templates to match. If you plan to use the new fields, you must correct the template mismatch by running the IRRMIN00 utility on the downlevel node, then IPL that node. Remember to upgrade the RACF dynamic parse specification data set (IRRDPDS) to match the template level. When the template levels match, you will no longer see this message when the two nodes TARGET each other.

Destination:  Descriptor code is 4. Routing codes are 2 and 9.

**IRRI005I**  ATTENTION: LOCAL NODE local-node  
[SYSNAME system-name] HAS  
DYNAMIC PARSE VERSION xxxxxx.  
PARTNER NODE partner-node  
[SYSNAME system-name] HAS  
DYNAMIC PARSE VERSION xxxxxx.

Explanation:  This is an attention message only. You can choose whether to act immediately. RACF checks certain data between the partner node and the local node to determine whether a command could run on one node but not the other. The dynamic parse specification data (IRRDPDS) level is one of these
types of data and a mismatch has been detected. Adding a profile segment field on one node may work, but fail on the other node until the corresponding dynamic parse specification update takes place on that node. If SYSNAME information is present for one or both of the nodes in this message, the node that precedes the SYSNAME is a multisystem node.

This message also occurs if dynamic parse initialization has not completed on both nodes. The dynamic parse version displayed for a node that has not completed dynamic parse initialization is '<UNKNOWN>'.

**System action:** If no error messages are issued with this node pair into the OPERATIVE ACTIVE state. Message IRRI0001I confirms when the OPERATIVE ACTIVE state is reached.

**System programmer response:** Evaluate the dynamic parse levels in the message. If you do not plan to add or alter a profile specifically using the segment fields that exist in the more recent version of the IRRDPDS, you may ignore this message until the next service upgrade causes the members to match. If you plan to use the new fields, you must correct the IRRDPDS mismatch by running the IRRDPDS UPDATE command on the downlevel node. Remember to upgrade the RACF templates to match the dynamic parse level. When the IRRDPDS levels match, you will no longer see this message when the two nodes TARGET each other.

If this message occurred because dynamic parse initialization did not complete on both nodes, dynamic parse initialization can be performed before starting the RACF address space to reduce the likelihood of this message appearing. After dynamic parse has completed on both nodes, SET LIST can be issued on each node to display the dynamic parse level. Alternatively, a command such as `TARGET NODE(local-node) OP that causes RACF to re-examine dynamic parse levels on both nodes can be issued. If the dynamic parse levels do not match, message IRRI005I is displayed again.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.

---

**IRR006I**

**ATTENTION: LOCAL NODE local-node HAS SETROPTS OPTION option. PARTNER NODE partner-node HAS SETROPTS OPTION option.**

**Explanation:** This is a warning message only. You can choose whether to act immediately. RACF checks certain data between the partner node and the local node to determine whether a command could run on one node but not the other. The indicated SETROPTS option is one of these types of data and a mismatch has been detected. Adding a profile on one node may work, but fail on the other node until the corresponding SETROPTS options match.

**System action:** If no error messages are issued with this warning message, RACF still attempts to move this node pair into the OPERATIVE ACTIVE state. Message IRRI0001I tells you when the OPERATIVE ACTIVE state is reached.

**System programmer response:** Evaluate the SETROPTS options in the message. These SETROPTS options must match when you want two RACF nodes to communicate with each other. You should use the SETROPTS command to change one or both nodes so that the SETROPTS options match. When the SETROPTS options match, you will no longer see this message when the two nodes TARGET each other.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.
**IRRI011I • IRRI014I**

**IRRI011I**

**ERROR: LOCAL NODE** local-node

[SYSNAME system-name] HAS RACF LEVEL xxxxx. PARTNER NODE partner-node [SYSNAME system-name] HAS RACF LEVEL xxxxx.

**Explanation:** This is an error message. The RACF levels at local node local-node and its partner node partner-node are not compatible. Each node must be at RACF 2.2 or higher in order for communication to occur between the nodes. If SYSNAME information is present for one or both of the nodes in this message, the node that precedes the SYSNAME is a multisystem node.

**System action:** Because this is an error, RACF does not move this node pair into the OPERATIVE ACTIVE state, but leaves them in an OPERATIVE PENDING VERIFICATION state. Message IRRI013I indicates RACF is not communicating with the partner node.

**System programmer response:** Evaluate the RACF levels in the message. Upgrade your RACF level and try the request again. See z/OS Security Server RACF System Programmer’s Guide for additional information. When the RACF levels match at RACF 2.2 or higher, you will no longer see this message when the two nodes TARGET each other, and communication should be allowed between the nodes.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.

**IRRI014I**

**ERROR: LOCAL NODE** node-name

[SYSNAME system-name] AND PARTNER NODE node-name [SYSNAME system-name] HAVE CONFLICTING TARGET STATEMENTS WITH (LOCAL | REMOTE) LUNAME luname. REASON CODE reason-code.

**Explanation:** RACF has successfully made a connection between the local node and a remote LU name. However, there is an inconsistency in the TARGET statements on the local and remote sides about which one of the LU names reference. The text of this message indicates the LU name in conflict and the reason code indicates the inconsistency. The reason code is one of these values:

<table>
<thead>
<tr>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>There is no agreement on node-name.</td>
</tr>
<tr>
<td>2</td>
<td>There is no agreement if a node is a multisystem node or a single-system node.</td>
</tr>
<tr>
<td>3</td>
<td>There is no agreement on system-name.</td>
</tr>
<tr>
<td>4</td>
<td>There is no agreement if the system on the multisystem node is the MAIN system.</td>
</tr>
</tbody>
</table>

**System action:** Because these are errors, RACF will not move this node pair into the OPERATIVE-ACTIVE state.
state. Instead they remain in an OPERATIVE-PENDING-VERIFICATION state. Message IRR0103I is received indicating that RACF does not communicate with the partner node.

**Operator response:** Do the following tasks:
- Issue the TARGET LIST command from both nodes and determine the error. If a node is multisystem, ensure that the TARGET LIST command is done from the specific system involved.
- Issue the TARGET DELETE command for the incorrect node definitions and TARGET the correct ones. If a node is multisystem, ensure that the corrections are made on every system.
- Ensure that corresponding updates are made to the RACF parameter library for future refreshes of the subsystem or reIPLs.

**Destination:** Descriptor code is 6. Routing code is 2.

**IRR015I**  
ERROR: HANDSHAKING HAS ALREADY FAILED ON PARTNER RRSF NODE node-name [SYSNAME system-name].

**Explanation:** An attempt has already been made to make this partner RRSF node operative and handshaking failed. Handshaking is not reattempted.

**System action:** These two nodes are left in the OPERATIVE-PENDING-VERIFICATION state. Communication is not allowed between these two nodes.

**System programmer response:** Refer to any preceding RACF error messages to determine what was incompatible between the two nodes. If message IRR0141I or IRR0161I was issued, correct the problem and issue RESTART CONNECTION NODE(node-name) for the specific node or system. If a protocol mismatch is detected, the entire set of communication tasks must be restarted to reload all handshaking modules. This can be done by issuing RESTART CONNECTION without the NODE keyword. If incompatible RACF levels are detected, an IPL is required after upgrading to a compatible RACF level to correct the problem.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.

**IRR0161**  
ERROR: LOCAL NODE node-name [SYSNAME system-name] AND PARTNER NODE node-name [SYSNAME system-name] HAVE CONFLICTING TARGET STATEMENTS WITH THE [LOCAL | REMOTE] SYSTEM.  
REASON CODE reason-code.

**Explanation:** RACF successfully made a connection between the local node and a remote RRSF node. However, there is an inconsistency in the TARGET statements on the local and remote nodes. The text of this message indicates the node and system name in conflict and the reason code indicates the inconsistency. The reason code is one of these values:

**Reason**
- 1 There is no agreement on a node name. This can occur normally when adding a new node that has not yet been defined using the TARGET command on the remote system.
- 2 There is no agreement if a node is a multisystem node or a single-system node.
- 3 There is no agreement on system-name.
- 4 There is no agreement if the system on the multisystem node is the MAIN system.
- 5 There is no agreement about the transport protocol being used for the connection.

**System action:** Because these are errors, RACF does not move this node pair into the OPERATIVE-ACTIVE state. Instead they are left in an OPERATIVE-PENDING-VERIFICATION state. Message IRR0103I is displayed and indicates that RACF does not communicate with the partner node.

**Operator response:** Do the following tasks:
- Issue the TARGET LIST command from both nodes and determine the error. If a node is multisystem, ensure that the TARGET LIST command is issued from the specific system involved.
- Issue the TARGET DELETE command for the incorrect node definitions and issue TARGET commands to define the deleted nodes correctly. If a node is multisystem, ensure that the corrections are made on every system.
- Ensure that corresponding updates are made to the RACF parameter library for future refreshes of the subsystem or reIPLs.

**Destination:** Descriptor code is 6. Routing code is 2.

**IRR020I**  
RRSF CONNECTION (TO | FROM) system-identifier HAS BEEN REJECTED DUE TO INSUFFICIENT AT-TLS POLICY. AT-TLS IS NOT ENABLED ON THE STACK.

**Explanation:** RACF remote sharing requires its connections, using the TCP protocol, be covered by an AT-TLS rule. It is AT-TLS that provides the authentication of RRSF nodes to one another, and encryption of traffic across the network. There is no rule covering this RRSF connection because AT-TLS was not enabled on the TCP/IP stack, or the Policy Agent, which serves the AT-TLS policy to TCP/IP, has not completed initialization when AT-TLS policy mapping was performed. The last case should not typically happen, as the listener should wait for the Policy Agent to initialize before allowing remote connection attempts to occur. However, if you have incorrectly permitted the RACF subsystem user ID to the EZB.INITSTACK.sysname.tcpname resource in the SERVAUTH class, this message is issued for any remote connection that is attempted before the Policy Agent
serves the policy to TCP/IP. See z/OS Security Server RACF System Programmer’s Guide for more information about AT-TLS.

The value for direction can be TO, when the message is issued by the system that initiated the connection, or FROM, when the message is issued by the system that received the connection request.

When the value of direction is TO, system-identifier is expressed as NODE node-name, followed by SYSNAME system-name, if the target is a multisystem node.

When the value of direction is FROM, the communication failed before RRSF identified the peer RRSF node and system name, or determined if the peer is a valid RRSF node. Therefore, system-identifier is expressed as PEER, followed by an IP address and a port number, separated by a colon. If necessary, you can use the z/OS UNIX host command shipped by z/OS UNIX System Services to map the IP address to a host name. See z/OS Communications Server: IP System Administrator’s Commands for more information about the z/OS UNIX host command. For example, if the peer information displayed is 1.2.3.4:1026, issue the following command:

$ host 1.2.3.4
EZB321I zossys1.xyz.com 1.2.3.4

**System action:** The connection is rejected. The RRSF connection is placed in the OPERATIVE-PENDING-VERIFICATION state.

**RACF Security Administrator Response:** Implement AT-TLS policy for this connection, or remove the RACF subsystem’s access list entry from the EZB.INITSTACK.sysname.tcpname profile in the SERVAUTH class. See z/OS Security Server RACF System Programmer’s Guide for information about RACF requirements.

**System programmer response:** After the security administrator has updated the AT-TLS policy, try the connection again with the TARGET OPERATIVE command for the failed node and system.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.

---

**IRR021I**

**RRSF CONNECTION (TO | FROM)**

**system-identifier HAS BEEN REJECTED DUE TO INSUFFICIENT AT-TLS POLICY. NO MATCHING POLICY RULE WAS FOUND.**

**Explanation:** RACF remote sharing requires its connections to be covered by an AT-TLS rule. It is AT-TLS that provides the authentication of RRSF nodes to one another, and encryption of traffic across the network. No matching policy rule was found when AT-TLS policy mapping was performed for the connection. See z/OS Security Server RACF System Programmer’s Guide for more information about AT-TLS.

The value for direction can be TO, when the message is issued by the system that initiated the connection, or FROM, when the message is issued by the system that received the connection request.

When the value of direction is TO, system-identifier is expressed as NODE node-name, followed by SYSNAME system-name if the target is a multisystem node.

When the value of direction is FROM, the communication failed before RRSF identified the peer RRSF node and system name, or determined if the peer is a valid RRSF node. Therefore, system-identifier is expressed as PEER, followed by an IP address and a port number, separated by a colon. If necessary, you can use the z/OS UNIX host command shipped by z/OS UNIX System Services to map the IP address to a host name. See z/OS Communications Server: IP System Administrator’s Commands for more information about the z/OS UNIX host command. For example, if the peer information displayed is 1.2.3.4:1026, issue the following command:

$ host 1.2.3.4
EZB321I zossys1.xyz.com 1.2.3.4

**System action:** The connection is rejected. The RRSF connection is placed in the OPERATIVE-PENDING-VERIFICATION state.

**RACF Security Administrator Response:** Implement AT-TLS policy for this connection. See z/OS Security Server RACF System Programmer’s Guide for information about RACF requirements.

**System programmer response:** After the security administrator has updated the AT-TLS policy, try the connection again with the TARGET OPERATIVE command for the failed node and system.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.

---

**IRR022I**

**RRSF CONNECTION (TO | FROM)**

**system-identifier HAS BEEN REJECTED DUE TO INSUFFICIENT AT-TLS POLICY. THE AT-TLS RULE NAME rule-name IS DISABLED.**

**Explanation:** RACF remote sharing requires its connections to be covered by an AT-TLS rule. It is AT-TLS that provides the authentication of RRSF nodes to one another, and encryption of traffic across the network. The policy rule that matches this connection (the TLSSRule named rule-name) indicates that AT-TLS should not be used. See z/OS Security Server RACF System Programmer’s Guide for more information about AT-TLS.

The value for direction can be TO, when the message is issued by the system that initiated the connection, or FROM, when the message is issued by the system that...
received the connection request.

When the value of direction is TO, system-identifier is expressed as NODE node-name, followed by SYSNAME system-name if the target is a multisystem node.

When the value of direction is FROM, the communication failed before RRSF identified the peer RRSF node and system name, or determined if the peer is a valid RRSF node. Therefore, system-identifier is expressed as PEER, followed by an IP address and a port number, separated by a colon. If necessary, you can use the z/OS UNIX host command to map the IP address to a host name. See z/OS Communications Server: IP System Administrator’s Commands for more information about the z/OS UNIX host command. For example, if the peer information displayed is 1.2.3.4:1026, issue the following command:

```bash
$ host 1.2.3.4
```

**System action:** The connection is rejected. The RRSF connection is placed in the OPERATIVE-PENDING-VERIFICATION state.

**RACF Security Administrator Response:** Implement AT-TLS policy for this connection and enable the rule. Also, review the AT-TLS policy and ensure that the TTLSEnabled flag, in the TTLGroupAction statement for the RRSF server and client, rules are set to ON. See z/OS Security Server RACF System Programmer’s Guide for information about RACF requirements.

**System programmer response:** After the security administrator has updated the AT-TLS policy, try the connection again with the TARGET OPERATIVE command for the failed node and system.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.

---

**IRRI023I** RRSF CONNECTION {TO | FROM} 

```
rule-name
```

HAS BEEN REJECTED 
DUE TO INSUFFICIENT AT-TLS POLICY. THE AT-TLS RULE NAME rule-name SPECIFIES APPLICATION CONTROL.

**Explanation:** RACF remote sharing requires its connections to be covered by an AT-TLS rule. It is an AT-TLS that provides the authentication of RRSF nodes to one another, and encryption of traffic across the network. The policy rule that matches this connection (the TTLSEnabled flag named rule-name) indicates AT-TLS is enabled for this connection, but that the application is responsible for initiating the secure handshake. RRSF does not provide support for this, instead RRSF relies on TCP/IP to establish the secure connection on the behalf of RRSF. See z/OS Security Server RACF System Programmer’s Guide for more information about AT-TLS.

If the ApplicationControlled keyword is present in the AT-TLS policy information for the RRSF client or server rule, make sure that the value is set to OFF.

---

**IRRI024I** RRSF CONNECTION {TO | FROM} 

```
rule-name
```

HAS BEEN REJECTED 
DUE TO INSUFFICIENT AT-TLS POLICY. THE AT-TLS RULE NAME rule-name DOES NOT CORRECTLY SPECIFY CLIENT AUTHENTICATION.

**Explanation:** RACF remote sharing requires its connections to be covered by an AT-TLS rule. It is an AT-TLS that provides the authentication of RRSF nodes to one another, and encryption of traffic across the network. The policy rule that matches this connection (the TTLSEnabled flag named rule-name) does not require client authentication. See z/OS Security Server RACF System Programmer’s Guide for more information about AT-TLS.

In the AT-TLS policy information for the RRSF server rule, make sure that the HandshakeRole keyword is set to ServerWithClientAuth and that the ClientAuthType keyword, if specified, is either Required (the default, if not specified) or SAFCheck.

The value for direction can be TO, when the message is issued by the system that initiated the connection, or FROM, when the message is issued by the system that received the connection request.

When the value of direction is TO, system-identifier is expressed as NODE node-name, followed by SYSNAME system-name if the target is a multisystem node.

When the value of direction is FROM, the communication failed before RRSF identified the peer RRSF node and system name, or determined if the peer is a valid RRSF node. Therefore, system-identifier is expressed as PEER, followed by an IP address and a port number, separated by a colon. If necessary, you can use the z/OS UNIX host command to map the IP address to a host name. See z/OS Communications Server: IP System Administrator’s Commands for more information about the z/OS UNIX host command. For example, if the peer information displayed is 1.2.3.4:1026, issue the following command:

```bash
$ host 1.2.3.4
```

**System action:** The connection is rejected. The RRSF connection is placed in the OPERATIVE-PENDING-VERIFICATION state.

**RACF Security Administrator Response:** Turn off the application-controlled indicator in the policy definition. See z/OS Security Server RACF System Programmer’s Guide for information about RACF requirements.

**System programmer response:** After the security administrator has updated the AT-TLS policy, try the connection again with the TARGET OPERATIVE command for the failed node and system.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.

---

Chapter 6. IRR messages for commands, utilities, and other tasks 305
Make sure that the HandshakeRole keyword is set to ServerWithClientAuth and that the ClientAuthType keyword, if specified, is either Required (the default, if not specified) or SAFCheck.

The value for direction can be TO, when the message is issued by the system that initiated the connection, or FROM, when the message is issued by the system that received the connection request.

When the value of direction is TO, system-identifier is expressed as NODE node-name, followed by SYSNAME system-name if the target is a multisystem node.

When the value of direction is FROM, the communication failed before RRSF identified the peer RRSF node and system name, or determined if the peer is a valid RRSF node. Therefore, system-identifier is expressed as PEER, followed by an IP address and a port number, separated by a colon. If necessary, you can use the z/OS UNIX host command to map the IP address to a host name. See z/OS Communications Server: IP System Administrator's Commands for more information about the z/OS UNIX host command. For example, if the peer information displayed is 1.2.3.4:1026, issue the following command:

$ host 1.2.3.4
EZZ8321I zossys1.xyz.com 1.2.3.4

System action: The connection is rejected. The RRSF connection is placed in the OPERATIVE-PENDING-VERIFICATION state.

RACF Security Administrator Response: The client authentication level must be set to at least "required". See z/OS Security Server RACF System Programmer’s Guide for information about RACF requirements.

System programmer response: After the security administrator has updated the AT-TLS policy, try the connection again with the TARGET OPERATIVE command for the failed node and system.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

rule, make sure that the HandshakeRole keyword is set to ServerWithClientAuth and that the ClientAuthType keyword, if specified, is either Required (the default, if not specified) or SAFCheck.

The value for direction can be TO, when the message is issued by the system that initiated the connection, or FROM, when the message is issued by the system that received the connection request.

When the value of direction is TO, system-identifier is expressed as NODE node-name, followed by SYSNAME system-name if the target is a multisystem node.

When the value of direction is FROM, the communication failed before RRSF identified the peer RRSF node and system name, or determined if the peer is a valid RRSF node. Therefore, system-identifier is expressed as PEER, followed by an IP address and a port number, separated by a colon. If necessary, you can use the z/OS UNIX host command to map the IP address to a host name. See z/OS Communications Server: IP System Administrator’s Commands for more information about the z/OS UNIX host command. For example, if the peer information displayed is 1.2.3.4:1026, issue the following command:

$ host 1.2.3.4
EZZ8321I zossys1.xyz.com 1.2.3.4

System action: The connection is rejected. The RRSF connection is placed in the OPERATIVE-PENDING-VERIFICATION state.


System programmer response: After the security administrator has updated the AT-TLS policy, try the connection again with the TARGET OPERATIVE command for the failed node and system.

Destination: Descriptor code is 4. Routing codes are 2 and 9.
When the value of direction is TO, system-identifier is expressed as NODE node-name, followed by SYSNAME system-name if the target is a multisystem node.

When the value of direction is FROM, the communication failed before RRSF identified the peer RRSF node and system name, or determined if the peer is a valid RRSF node. Therefore, system-identifier is expressed as PEER, followed by an IP address and a port number, separated by a colon. If necessary, you can use the z/OS UNIX host command to map the IP address to a host name. See z/OS Communications Server: IP System Administrator’s Commands for more information about the z/OS UNIX host command. For example, if the peer information displayed is 1.2.3.4:1026, issue the following command:

$ host 1.2.3.4
EZZ8321I zossys1.xyz.com 1.2.3.4

System action: The connection is rejected. The RRSF connection is placed in the OPERATIVE-PENDING-VERIFICATION state.

RACF Security Administrator Response: See z/OS UNIX System Services Messages and Codes for more information about return codes (errnos). Try to determine the cause and fix it. If you are unable to determine the cause, contact IBM service.

System programmer response: After the condition has been fixed, try the connection again with the TARGET OPERATIVE command for the failed node and system.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRI0027I  RRSF CONNECTION FROM PEER
type HAS BEEN REJECTED
BECAUSE OF AN AUTHORIZATION
FAILURE DURING CLIENT
AUTHENTICATION CHECKING.

Explanation: The AT-TLS rule covering this RACF remote sharing connection specifies a client authentication level of SAFCheck. AT-TLS successfully mapped the digital certificate of the remote partner to a local RACF user ID, and RRSF retrieved the user ID value. This user ID cannot be successfully verified, or the user does not have at least READ access to the IRR.RRSF.CONNECT resource in the RRSFDATA class. An ICH408I message describing the failure is displayed on the console before this one.

The communication failed before RRSF identified the peer RRSF node and system name, or even determine if the peer is a valid RRSF system. The peer-info is expressed as an IP address and a port number, separated by a colon. If necessary, use z/OS UNIX host command to map the IP address to a host name. For example, if the peer information displayed is 1.2.3.4:1026, issue the following command:

$ host 1.2.3.4
EZZ8321I zossys1.xyz.com 1.2.3.4

System action: The connection is rejected. The RRSF connection is placed in the OPERATIVE-PENDING-VERIFICATION state.

RACF Security Administrator Response: Fix the mapped user ID, or grant it access to IRR.RRSF.CONNECT.

System programmer response: After the underlying problem is fixed by the security administrator, try the connection again with the TARGET OPERATIVE command for the failed node and system.

Destination: Descriptor code is 4. Routing codes are 2 and 9.
IRRI030I RRSF CONNECTION [TO | FROM] system-identifier HAS BEEN REJECTED BECAUSE RACF COULD NOT VERIFY AT-TLS POLICY. THE service-name SERVICE TIMED OUT.

Explanation: RACF remote sharing requires its connections to be covered by an AT-TLS rule. It is AT-TLS that provides the authentication of RRSF nodes to one another, and encryption of traffic across the network. RRSF uses the select() service (BPX1SEL) to force the underlying TLS handshake to occur so that the AT-TLS policy for this connection can be verified. The select() returned with a socket exception.

There might be a setup error with AT-TLS policy or with the underlying key ring and digital certificates. See the AT-TLS errors section in z/OS Security Server RACF Diagnosis Guide for more information about what you can check. If you cannot determine the cause of the error, contact IBM service. You might find helpful information for IBM service in the AT-TLS trace records on both the local and remote systems.

The value for direction can be TO, when the message is issued by the system that initiated the connection, or FROM, when the message is issued by the system that received the connection request.

When the value of direction is TO, system-identifier is expressed as NODE node-name, followed by SYSNAME system-name if the target is a multisystem node.

When the value of direction is FROM, the communication failed before RRSF identified the peer RRSF node and system name, or even determine if the peer is a valid RRSF system. Therefore, system-identifier is expressed as PEER followed by an IP address and a port number, separated by a colon. If necessary, you can use the z/OS UNIX host command to map the IP address to a host name. For example, if the peer information displayed is 1.2.3.4:1026, issue the following command:

```bash
$ host 1.2.3.4
EZZ8321I zossys1.xyz.com 1.2.3.4
```

System action: The connection is rejected. RRSF places the connection into the OPERATIVE-PENDING-VERIFICATION state.

RACF Security Administrator Response: Look for AT-TLS trace records to see if the problem is related to AT-TLS policy setup. If so, fix the issue. If you are unable to determine the cause, contact IBM service.

System programmer response: After the condition has been fixed, try the connection again with the TARGET OPERATIVE command for the failed node and system.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRI080I subsystem-name SUBSYSTEM APPC HANDSHAKING TASK HAS ENCOUNTERED AN ERROR. ABEND CODE IS abend-code.

Explanation: The handshaking task was processing conversation connection parameters. This message is
displayed when an abnormal event occurs.

**System action:** The handshaking task attempts to try the current work request again. If that does not work, message IRRI081I is issued.

**Operator response:** Report the occurrence of the message to the system programmer.

**Problem Determination:** For an explanation of these codes, see [z/OS MVS System Codes](https://www.ibm.com/support/knowledgecenter/SSEPGG_2.4.0/com.ibm.zos.r24.sicmvs.zz.pdf).

**Destination:** Descriptor code is 1. Routing codes are 2 and 9.

---

IRRI081I subsystem-name SUBSYSTEM APPC HANDSHAKING TASK HAS ENCOUNTERED AN ERROR. ABEND CODE IS abend-code. HANDSHAKING TASK ENDING.

**Explanation:** The handshaking task was processing conversation connection parameters. This message is displayed when an abnormal event occurs.

**System action:** The handshaking subtask ends and the parent task attempts to restart the handshaking subtask.

**Operator response:** Report the occurrence of the message to the system programmer.

**Problem Determination:** For an explanation of these codes, see [z/OS MVS System Codes](https://www.ibm.com/support/knowledgecenter/SSEPGG_2.4.0/com.ibm.zos.r24.sicmvs.zz.pdf).

**Destination:** Descriptor code is 6. Routing code is 2.
RRSF connection local transaction program messages

IRRJ000I subsystem-name RACF LOCAL NODE TRANSACTION PROGRAM STARTING UNDER USER ID userid GROUP group-name.

Explanation: This message goes to the SYSLOG when the local node transaction program completes its initialization. The local RACF subsystem can process commands sent to it for processing on the local system.

IRRJ001I subsystem-name RACF LOCAL NODE TRANSACTION PROGRAM COMPLETED UNDER USER ID userid GROUP group-name.

Explanation: This message goes to the SYSLOG when the local node transaction program stops processing. The program may be stopped as a result of an operator request to make the node dormant or as the result of an operational error. Earlier messages may indicate the nature of the problem.

System action: The RACF subsystem does not run any local work until the node is returned to operative active status. Additional RACF commands directed to the local node are held in the local OUTMSG workspace data set. Work (commands and other requests) active in the RACF address space continue to run. Work directed to other nodes continues to be processed if the target node is operative active.

Operator response: Review the console log for an indication of the original error.

IRRJ080I subsystem-name RACF LOCAL NODE TRANSACTION PROGRAM ENCOUNTERED AN ERROR. ABEND CODE IS abend-code.

Explanation: A local node transaction program handling work requests to run in the RACF subsystem had an error. This message is displayed when the program encounters an abnormal event that cannot be recovered from.

System action: The transaction program cannot recover from this abnormal error. The program releases all system resources it holds and then ends. The node connection program attempts to restart the local transaction program.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. See “Actions to Recover from an RRSF Failure” in z/OS Security Server RACF Diagnosis Guide for a complete discussion.

Operator response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see z/OS MVS System Codes.

IRRJ081I subsystem-name RACF LOCAL NODE TRANSACTION PROGRAM ENCOUNTERED AN ERROR. ABEND CODE IS abend-code. PROGRAM ENDING.

Explanation: A local node transaction program handling work requests to run in the RACF subsystem had an error. This message is displayed when the program encounters an abnormal event that cannot be recovered from.

System action: The transaction program cannot recover from this abnormal error. The program releases all system resources it holds and then ends. The node connection program attempts to restart the local transaction program.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. See “Actions to Recover from an RRSF Failure” in z/OS Security Server RACF Diagnosis Guide for a complete discussion.

Operator response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see z/OS MVS System Codes.

Destination: Descriptor code is 6. Routing code is 2.
RACLINK command messages

IRRK080I subsystem-name SUBSYSTEM RACLINK TASK HAS ENCOUNTERED AN ERROR. ABEND CODE IS abend-code.

Explanation: The RACF subsystem RACLINK task has abended for the indicated subsystem. This message is written to the SYSLOG.

System action: The RACF subsystem continues processing without this RACLINK task.

Operator response: Take the steps indicated by for z/OS MVS System Codes the abend and reason code that was displayed when the subtask abended. When the problem is resolved, restart the RACLINK subtask by using the RESTART command.
RACROUTE REQUEST=LIST messages

**IRRL0000I** Error occurred while processing RACGLIST profile `classname_nnnnn`, error code = `error`, RACF manager return code = `retcode`, reason code = `rsncode`.

**Explanation:** While RACF was processing RACGLIST profiles, an error was encountered while processing the `classname_nnnnn` profile. `Error` uniquely identifies where in RACF the problem was discovered.

**System action:**
- If the problem occurred while RACF was building a RACTION data space from the RACGLIST profiles, RACF reverts to standard RACTION processing, which loads the original class profiles from the database into a data space instead of using the RACGLIST profiles. The RACGLIST `classname_nnnnn` profiles are rebuilt.
- If the problem occurred while saving the RACTION data space contents on the database as RACGLIST profiles, RACTION processing has created the data space successfully, but the contents were not saved as RACGLIST profiles. An attempt is made to delete all `classname_nnnnn` profiles from the RACF database. If a second IRRL0000I message is not issued, the attempt was successful and all but the base `classname` profile were deleted.
- If the problem occurred while deleting the RACGLIST profiles, for example, during a SETR NORACLST or RDELETE command, all the RACGLIST profiles may not have been deleted.

In all cases, an SVC dump is taken.

**Operator response:** Notify the system programmer.

**System programmer response:**
1. Look up RACF manager return and reason codes in "RACF manager return codes" on page 405 to determine the cause.
2. Issue SEARCH CLASS(RACGLIST) to determine the status of the RACGLIST profiles.
3. Issue a SETROPTS RACTION REFRESH for the indicated `classname` to rebuild RACGLIST profiles. If the problem persists, report the problem to the IBM support center for further problem analysis.

**Destination:** Descriptor code is 6. Routing code is 2.

**IRRL0002I** RACROUTE REQUEST=LIST for `classname` failed to build or return a data space, error code = `error`.

**Explanation:** A RACROUTE REQUEST=LIST, GLOBAL=YES, for class `classname` has failed. The error code uniquely identifies where in RACF the problem was discovered.

**System action:** The RACTION failed with SAF return code = X'8', RACF return code = X'24', RACF reason code = X'0'. Under some circumstances, an SVC dump is taken.

**Operator response:** Notify the system programmer.

**System programmer response:** Report the problem to the IBM support center for further problem analysis.

**Destination:** Descriptor code is 6. Routing code is 2.

**IRRL0003I** RACLIST of class `classname` failed.

```
Profile | Grouping Class Profile | Group Member
```

`pname` is too large.

**Explanation:** While processing a SETROPTS RACTION [REFRESH] or RACROUTE REQUEST=LIST request for a class, the in-storage profile `pname` being built from one of the following was too large to be RACLISTed:

- A profile in class `classname`
- A profile in the grouping class associated with `classname`
- A member of one or more grouping class profiles associated with `classname`

If `pname` is followed by the notation '(G)', it is a generic profile.

**System action:** The RACTION [REFRESH] request failed with SAF return code = X'8', RACF return code = X'0C', RACF reason code = X'00'.

**User response:** The in-storage profile `pname` was too large to be RACLISTed.

If the profile is defined to RACF in more than one way, for example, as a member of a grouping class profile...
and as a profile in the corresponding member class, RACF merges the multiple definitions to form a resulting in-storage profile. It may be the combination of the two or more definitions of the profile, not the individual definitions themselves, that caused the profile to be too large.

If \textit{pname} is identified as a group member in the message, you can issue the RLIST \textit{classname} \textit{pname} RESGROUP command to locate all the grouping class profiles that have it as a member.

Decrease the size of the profile (or its associated profiles). The standard and conditional access lists are the most likely areas to cause the profile to grow. Other areas to consider are the installation data, the application data, or categories.

After you have made the profile smaller, reissue the SETROPTS RACLIST command or have the application reissue the RACROUTE REQUEST=LIST request. If the profile is generic, issue the SETROPTS GENERIC(\textit{classname}) REFRESH command.

**Note:** If you are not responsible for administering those profiles, you should contact the RACF security administrator.

For more information about the size restriction of an in-storage profile, see section in the \textit{z/OS Security Server RACF Security Administrator's Guide} on “Limiting the Size of Your Access Lists”.

**Operator response:** Report this message to the RACF security administrator.

**System programmer response:** See User Response.

**Destination:** Descriptor code is 6. Routing codes are 2 and 11.

---

**CACHECLS profile messages**

**IRRL1000I** Cache is intact. Error occurred while processing CACHECLS profile

\textit{profile-name}, error code = \textit{error}, RACF manager return code = \textit{retcode}, reason code = \textit{rsncode}.

**Explanation:** An R\_cacheserv callable service was invoked. During the hardening of the cache contents to the RACF database as CACHECLS profiles, an error occurred while processing profile \textit{profile-name}. \textit{Profile-name} is in the format of either \textit{cachename} or \textit{cachename_ddd_nnnnn}, where \textit{cachename} is the value of the Cache Name parameter on the \textit{R\_Cacheserv} callable service. \textit{ddd} and \textit{nnnnn} are the dataspace number and sequential number respectively (both in decimal) of one of the profiles holding the contents of that particular dataspace. \textit{Error} is provided to assist IBM support personnel in identifying where in RACF the problem was discovered. RACF manager return and reason codes (in hexadecimal) are also provided to further delineate the problem.

The local cache is intact, but may not have been hardened to the database correctly. The application using the cache should not be affected now, but after an IPL it may not be possible to restore the cache from information about the RACF database. In that case, the application would not have use of the cache until it was built by other means.

**System action:** RACF attempts to delete all the \textit{cachename_ddd_nnnnn} profiles. If message IRRL1002I is not issued, the attempt was successful. If an IRRL1002I message is issued, then all \textit{cachename_ddd_nnnnn} profiles may not have been deleted.

Additionally, a symptom record for the error is created and stored in the LOGREC data set.

**Operator response:** Notify the system programmer.

**System programmer response:**

1. Look up the RACF manager return and reason codes on page "RACF manager return codes" on page 405 to determine the cause of the problem.
2. Contact your Security Administrator to check the status of the \textit{cachename_ddd_nnnnn} profiles.

**RACF Security Administrator Response:** If IRRL1002I is issued, then:

- Issue SEARCH CLASS(CACHECLS) to determine the status of the CACHECLS \textit{cachename_ddd_nnnnn} profiles
- If some remain, delete those profiles with the RACF RDELETE command.
- If the problem persists, report the problem to the IBM Support Center for further problem analysis.

**Destination:** Descriptor code is 6. Routing code is 2.

**IRRL1001I** Cache is not created. Error occurred while processing CACHECLS profile

\textit{profile-name}, error code = \textit{error}, [RACF manager return code = \textit{retcode}, reason code = \textit{rsncode}]

**Explanation:** An R\_cacheserv callable service was invoked. When RACF was building a cache from profiles on the RACF database in the CACHECLS class, an error was encountered while processing profile \textit{profile-name}. \textit{Profile-name} is in the format of either \textit{cachename}, or \textit{cachename_ddd_nnnnn}, where \textit{cachename} is the value of the Cache_name parameter on the \textit{R\_Cacheserv} callable service \textit{ddd} and \textit{nnnnn} are the dataspace number and sequential number respectively (both in decimal) of one of the profiles holding the contents of that particular dataspace. \textit{Error} is provided to assist IBM support personnel in identifying where in RACF the problem was discovered. RACF manager...
IRRL1002I • IRRL1003I

return and reason codes (in hexadecimal) are provided if the problem was encountered while accessing the RACF database.

System action: The local cache is not created, which means that applications cannot use the cache. Also, an attempt was made to delete all cachename_ddd_nnnnn profiles from the RACF database. If an IRRL1002I message is not additionally issued, the attempt was successful and all cachename_ddd_nnnnn profiles have been deleted. If an IRRL1002I message is issued, then all cachename_ddd_nnnnn profiles may not have been deleted.

Additionally, a symptom record for the error is created and stored in the LOGREC data set.

Operator response: Notify the system programmer.

System programmer response:
• Look up the RACF manager return and reason codes on page "RACF manager return codes" on page 405 to determine the cause of the problem.
• Contact your Security Administrator to check the status of the cachename_ddd_nnnnn profiles.

RACF Security Administrator Response:
• Issue SEARCH CLASS(CACHECLS) to determine the status of the CACHECLS cachename_ddd_nnnnn profiles.
• If scope is in the 'ddd' format and '_nnnnn' profiles remain for that particular 'ddd' and cachename whose name is equal to or greater than the profile named in the message, attempt to delete them with the RACF RDELETE command.
• If the problem persists, report the problem to the IBM Support Center for further problem analysis.

Destination: Descriptor code is 6. Routing code is 2.

IRRL1002I Delete request problem. Error occurred while processing CACHECLS profile profile-name, scope = [ddd] | MULTI | ALL, error code = error, RACF manager return code = retcode, reason code = rsncode

Explanation: RACF was processing a request to delete CACHECLS profiles due to an RDELETE command or an R_cacheserv callable service invocation, and encountered an error while processing profile profile-name. Profile-name is in the format of either 'cachename', or 'cachename_ddd_nnnnn', where cachename is the value of the Cache_Name parameter on the R_cacheserv callable service. 'ddd' and 'nnnnn' are the data space number and sequential number (both in decimal) of one of the profiles holding the contents of that particular data space. The scope of the delete request is either 'ddd' indicating that only profiles for that specific data space were to be deleted; MULTI indicating that profiles from multiple data spaces from the 'ddd' within the profile name through to the last profile for 'cachename' were to be deleted; or 'ALL', indicating that the 'nnnnn' profiles for all the data spaces for 'cachename' were to be deleted. Error is provided to assist IBM support personnel in identifying where in RACF the problem was discovered. RACF manager return and reason codes (in hexadecimal) are also provided.

If the problem was encountered while processing an R_cacheserv callable service invocation, another IRRL100xI message may also have been issued indicating the status of the cache being processed.

If the problem was encountered while processing an R_cacheserv callable service invocation and none of those messages were issued, or the request resulted from an RDELETE command, the status of the local cache is not affected by this problem.

Operator response: Notify the system programmer.

System programmer response:
• Look up the RACF manager return and reason codes on page "RACF manager return codes" on page 405 to determine the cause of the problem.
• Contact your Security Administrator to check the status of the cachename_ddd_nnnnn profiles.

RACF Security Administrator Response:
• Issue SEARCH CLASS(CACHECLS) to determine the status of the CACHECLS cachename_ddd_nnnnn profiles.
• If scope is in the 'ddd' format and '_nnnnn' profiles remain for that particular 'ddd' and cachename whose name is equal to or greater than the profile named in the message, attempt to delete them with the RACF RDELETE command. If scope is 'MULTI' and any profiles remain for a data space equal to or greater than the 'ddd' within the profile, attempt to delete them. If scope is 'ALL' and any '_nnnnn' profiles remain for that cachename, attempt to delete them all.
• If the problem persists, report the problem to the IBM Support Center for further problem analysis.

Destination: Descriptor code is 6. Routing code is 2.

IRRL1003I Cache is not affected. Error occurred while processing CACHECLS profile profile-name, error code = error, RACF manager return code = retcode, reason code = rsncode.

Explanation: An R_cacheserv callable service was invoked to retrieve the version level of the cache. During an attempt to read the specified profile to determine if a local cache had been hardened to the database, and if so retrieve its version level, an error occurred. Profile-name is in the format of either 'cachename', or 'cachename_ddd_nnnnn', where cachename is the value of the Cache_Name parameter on the R_Cacheserv callable service. 'ddd' and 'nnnnn' are the data space number and sequential number respectively (both in decimal) of one of the profiles holding the contents of that particular data space. Error is provided to assist IBM support personnel in identifying where in
RACF the problem was discovered. RACF manager return and reason codes (in hexadecimal) are also provided to further delineate the problem.

The status of the local cache is not affected by this error: if the cache existed before the error it remains in existence. If a hardened version of the cache had existed on the RACF database as profiles in the CACHECLS class, this error results in an attempt to delete them.

**System action:** RACF attempts to delete all the *cachename_ddd_nnnnn* profiles. If message IRRL1002I is not issued, the attempt was successful. If an IRRL1002I message is issued, then all *cachename_ddd_nnnnn* profiles may not have been deleted.

Additionally, a symptom record for the error is created and stored in the LOGREC data set.

**Operator response:** Notify the system programmer.

### TARGET command messages

**IRRMO01I**  
*subsystem-name* SUBSYSTEM TARGET COMMAND ENDED IN RECURSIVE ABEND.

**Explanation:** The TARGET command abnormally ended in its attempt to recover from a prior abend on the indicated subsystem.

**System action:** None.

**Operator response:** Report the occurrence of the message to the system programmer.

**System programmer response:** Gather appropriate diagnostic information and contact the IBM support center.

**Destination:** Descriptor code is 6.

**IRRMO02I**  
*subsystem-name* SUBSYSTEM TARGET COMMAND HAS COMPLETED SUCCESSFULLY.

**Explanation:** The TARGET command was processed by the *subsystem-name* subsystem without encountering any errors.

**System action:** None.

**Operator response:** None.

**Destination:** Descriptor code is 6.

**IRRMO03I**  
*subsystem-name* SUBSYSTEM TARGET COMMAND ENDED IN ERROR. [THE NODE WAS CREATED].

**Explanation:** The TARGET command encountered an error during execution by the indicated subsystem. See any accompanying messages for more specific error information.

**System programmer response:**
1. Look up the RACF manager return and reason codes in Chapter 12, “RACF return codes,” on page 405 to determine the cause of the problem.
2. Contact your Security Administrator to check the status of the *cachename_ddd_nnnnn* profiles.

**Security Administrator:**
1. Issue SEARCH CLASS(CACHECLS) to determine the status of the CACHECLS *cachename_ddd_nnnnn* profiles.
2. If some remain, delete those profiles with the RACF RDELETE command.
3. If the problem persists, report the problem to the IBM support center for further problem analysis.

**Destination:** Descriptor code is 6. Routing code is 2.

For new nodes, the node might not have been created. The message indicates when a node has been created.

**System action:** None.

**Operator response:** Report the occurrence of the message to the system programmer.

**System programmer response:** Gather appropriate diagnostic information and contact the IBM support center if the accompanying error messages do not indicate user error.

**Destination:** Descriptor code is 6.

**IRRMO04I**  
*subsystem-name* SUBSYSTEM TARGET COMMAND WAS UNABLE TO OBTAIN STORAGE FOR NODE node-name SYSNAME system-name.

**Explanation:** A new node, *node-name*, cannot be defined by the TARGET command because of an unexpected storage shortage within the *subsystem-name* subsystem's address space.

**System action:** The TARGET command ends in error.

**Operator response:** Report the occurrence of the message to the system programmer.

**System programmer response:** Reissue the TARGET command to determine if the storage shortage condition is persistent.

**Problem Determination:** If the storage shortage condition is persistent, obtain a dump of the *subsystem-name* subsystem’s address space and contact the IBM support center.

**Destination:** Descriptor code is 6.
IRRMO05I • IRRMO09I

IRRMO05I subsystem-name SUBSYSTEM TARGET
COMMAND WAS UNABLE TO FIND
DEFINITION OF NODE node-name
[SYSNAME system-name][ PROTOCOL
protocol-name].

Explanation: The intended function could not be
processed for node node-name because the node (or its
specific system name or protocol instance) does not
appear to have been defined by a previous TARGET
command by the indicated subsystem.

System action: The TARGET command ends in error.
Operator response: This might indicate that an
incorrect node name was specified on the command.
Correct and reissue the command.
Destination: Descriptor code is 6.

IRRMO06I subsystem-name SUBSYSTEM TARGET
COMMAND HAS FOUND THAT THE
LOCAL NODE IS ALREADY DEFINED
AS node-name.

Explanation: An attempt to specify the LOCAL
keyword for a node is disallowed. The TARGET
command has found that a previous TARGET
command by the indicated subsystem defined
node-name to be the local node. Only one node may be
designated as the local node.

System action: The TARGET command ends in error.
Operator response: If the failing TARGET command
was issued during RACF parameter library processing,
this may indicate a logical error within parameter
library setup, such as the redundant or accidental
inclusion of a given member. Report such an error to
the system programmer. If the failing TARGET
command was issued manually, TARGET LIST may be
issued to display the defined nodes before proceeding
with any subsequent TARGET command issuances.

System programmer response: If a logical error within
the RACF parameter library setup is suspected,
determine the set of members processed and their
constituent commands. See z/OS Security Server RACF
Command Language Reference for a description of the
SET command and the SET INCLUDE() keyword and
its implications for the order of command execution (if appropriate).
Destination: Descriptor code is 6.

IRRMO07I subsystem-name SUBSYSTEM TARGET
COMMAND HAS FOUND THAT
NODE(*) OR SYSNAME(*) CONFLICTS
WITH ONE OR MORE SPECIFIED
KEYWORDS.

Explanation: NODE(*) is allowed only when the only
function requested is a listing or SYSNAME(*), but one
or more keywords other of the node definitions
specifying the LIST keyword. When SYSNAME(*) is
specified, the only other keywords allowed are
NODE(node-name), DORMANT, OPERATIVE, DELETE,
PURGE, or LIST. RACF detected a keyword other than
the ones allowed.

System action: The TARGET command ends in error.
Operator response: Correct and reissue the command.
Destination: Descriptor code is 6.

IRRMO08I subsystem-name SUBSYSTEM TARGET
COMMAND CANNOT DELETE
LOCAL NODE node-name [SYSNAME
system-name] [PROTOCOL protocol-name]
WHILE OTHER [protocol-name] NODES
ARE DEFINED.

Explanation: The TARGET command requires that the
local node is the last TARGET definition deleted.
Because this is not the case, the local node definition is
not deleted. The TARGET command requires that the
local member whose SYSNAME matches the
CVTSNAME is the last TARGET definition deleted.

If protocol information is displayed in the message, you
are attempting to delete the protocol instance from the
local node when there are remote nodes defined to use
that protocol. The local node protocol instance cannot
be deleted until all remote nodes using that protocol
are deleted.

System action: The TARGET command is ignored.
Operator response: If the local node is a single-system
node, first delete all remote nodes through appropriate
TARGET commands. If the local node is a multisystem
node, first delete all remote nodes and any member
systems of the local node through appropriate TARGET
commands, then reissue the command to delete the
local node. If a protocol instance is deleted from the
local node, first delete all remote nodes that use that
protocol. Note that the local node and the operative
remote nodes that are to be deleted must be made
dormant before their deletion.

Destination: Descriptor code is 6.

IRRMO09I [LOCAL | REMOTE] RRSF NODE
node-name [SYSNAME system-name]
[MAIN][ PROTOCOL protocol-name] IS
IN THE state STATE.

Explanation: This is an informational message only.
The state of the named node and system at the time of
the invocation of the TARGET command is as given. If
SYSNAME information is present in this message, the
node node-name is a multisystem node. If MAIN is
present in this message, the SYSNAME system-name is
the receiver of the RRSF network traffic directed to this
multisystem node. If PROTOCOL information is
present, then more than one protocol is defined for the
node, and this message pertains to the protocol
Explanation: This is an informational message only.
This message precedes the remainder of the output displayed for node node-name by TARGET LIST processing. If SYSNAME information is present in this message, the node node-name is a multisystem node and the information is displayed for system system-name of the named node. If MAIN is present in this message, the system-name is the receiver of the RRSF network traffic directed to this multisystem node. If PROTOCOL information is present, the node node-name has multiple protocol instances, and the information is displayed for the protocol-name protocol instance of the named node.

Operator response: None.

Destination: Descriptor code is 6.

IRRM010I subsystem-name SUBSYSTEM
PROPERTIES OF (LOCAL | REMOTE)
RRSF NODE node-name [SYSNAME
system-name] [(MAIN)] [ PROTOCOL
protocol-name]:

Explanation: This is an informational message only.
This message precedes the remainder of the output displayed for node node-name by TARGET LIST processing. If SYSNAME information is present in this message, the node node-name is a multisystem node and the information is displayed for system system-name of the named node. If MAIN is present in this message, the system-name is the receiver of the RRSF network traffic directed to this multisystem node. If PROTOCOL information is present, the node node-name has multiple protocol instances, and the information is displayed for the protocol-name protocol instance of the named node.

Operator response: None.

Destination: Descriptor code is 6.

IRRM011I subsystem-name SUBSYSTEM
COMMAND CANNOT MAKE NODE
node-name [SYSNAME system-name]
(OPERA TIVE | DORMANT) BECAUSE
ITS PROTOCOL IS UNKNOWN | ITS
LUNAME IS UNKNOWN | NO LOCAL
NODE OR SYSTEM IS DEFINED | ONE
OR MORE WORKSPACE FILES
COULD NOT BE ALLOCATED | A
PREFIX VALUE HAS NOT BEEN
SPECIFIED | NO LOCAL LUNAME IS
DEFINED | NO LOCAL MAIN IS
DEFINED | NO REMOTE MAIN IS
DEFINED | THE LOCAL NODE OR
SYSTEM IS IN THE INITIAL STATE).

Explanation: The state of node node-name is not changed for the reason given. If SYSNAME information is present in this message, the node node-name refers to a multisystem node and sysname system-name is a member system of that node.

Operator response: Issue TARGET commands to provide the missing information along with the [OPERATIVE | DORMANT] keyword, as appropriate.

Destination: Descriptor code is 6.

IRRM012I WARNING: SUBSYSTEM
subsystem-name IS OPERATING UNDER
A USERID THAT IS NOT PRIVILEGED
OR TRUSTED.

Explanation: This message is generated only when the first RACF remote sharing TARGET command is issued and the user ID associated with the RACF address space is not privileged or trusted. This user ID must be privileged or trusted, but does not require it.

System action: Processing continues.

System programmer response: The user ID associated with the RACF address space is not required to be privileged or trusted. However, if the user ID is not privileged or trusted, it must explicitly be given update access to all data sets used by RACF remote sharing facility (RRSF). Failure to do so results in access errors.

The user ID can be made privileged or trusted by activating the STARTED class and defining a profile for the user ID and specifying either privileged or trusted. The RACF address space must then be stopped and restarted. Alternatively, an entry for the user ID specifying either privileged or trusted can be made in the RACF started procedures table. However, the new entry does not take effect until the next IPL.

Destination: Descriptor code is 6.

IRRM013I subsystem-name SUBSYSTEM TARGET
COMMAND HAS FOUND THAT THE
PREFIX SPECIFIED FOR NODE
node-name [SYSNAME system-name]
EXCEEDS THE MAXIMUM LENGTH
OF number CHARACTERS.

Explanation: Prefix strings cannot exceed number characters because of workspace file naming conventions. The TARGET command has detected that the specified prefix exceeds this limit and does not update the prefix of node node-name. If SYSNAME information is present in this message, the node node-name is a multisystem node.

System action: The TARGET command ends in error.

Operator response: Correct and reissue the command.


Destination: Descriptor code is 6.

IRRM014I subsystem-name SUBSYSTEM TARGET
COMMAND CANNOT CHANGE THE
PREFIX VALUE FOR NODE
node-name [SYSNAME system-name]
BECAUSE ITS WORKSPACE FILES ARE ALREADY
ALLOCATED.

Explanation: The TARGET command has detected that one or more workspace data sets for node node-name are currently allocated and does not update the prefix of node node-name. A node’s prefix is used in the formation of workspace file names and is changeable until those files have been allocated, which normally occurs during processing of a DORMANT/OPERATIVE keyword. After the files have been allocated, it cannot
be changed. If SYSNAME information is present in this message, the node node-name is a multisystem node.

System action: The TARGET command ends in error.

Operator response: Issue the TARGET NODE(node-name) LIST command to view information for node node-name, including its prefix. If a different prefix for node node-name is required, delete the node and redefine it with the new prefix. Note that a new prefix value causes a new set of workspace data sets to be created for the node after it is reactivated. See z/OS Security Server RACF Command Language Reference for information about the TARGET command and the disposition of workspace data sets affected by DELETE keyword processing.

Destination: Descriptor code is 6.

Explanation: The TARGET command has detected that one or more workspace data sets for node node-name are currently allocated and does not update the workspace data set attributes for node node-name. A node’s workspace file attributes are changeable until the files have been allocated, which normally occurs during processing of a DORMANT/OPERATIVE keyword. After the files have been allocated, the file attributes may not be changed. If SYSNAME information is present in this message, the node node-name is a multisystem node.

System action: The TARGET command ends in error.

Operator response: Issue the TARGET NODE(node-name) LIST command to view information for node node-name, including its workspace file attributes. If different file attributes for node node-name are required, delete the node and redefine it with the new attributes. Note that new attributes might cause a new set of workspace files to be created for the node once it is reactivated. See z/OS Security Server RACF Command Language Reference for information about the TARGET command and the disposition of workspace data sets affected by DELETE keyword processing.

Destination: Descriptor code is 6.

Explanation: The TARGET command has detected an attempt to change the protocol information for a node that is in an operative state. The protocol information of a node is changeable only if the node is in the dormant state, except for LU name which can only be modified while the node is in the INITIAL state. If SYSNAME information is present in this message, the node node-name is a multisystem node.

System action: The TARGET command ends in error.

Operator response: Issue the TARGET LIST command to view a summary of the nodes and their current states. If the protocol information for node node-name must be changed, issue the TARGET NODE(node-name) DORMANT command to change the state and allow a reissuance of the failed TARGET command to succeed. The reissued command may include the OPERATIVE keyword or a subsequent TARGET NODE(node-name) OPERATIVE command may be issued to reactivate the node when appropriate.

Note: If you receive this message while listing the local node, issue the TARGET command again without the PROTOCOL keyword. When listing the local node, information for all defined protocols is automatically displayed.

Destination: Descriptor code is 6.

Explanation: Each node must have its own unique identifier pertaining to its defined protocol. For the APPC protocol, the identifier is the LU name. For the TCP protocol, the identifier is the host address.

System action: The TARGET command has detected an attempt to use an identifier that is currently associated with another node. The identifier for node node-name is not altered. If SYSNAME information is present in this message, the node node-name is a multisystem node.

Note: TCP host addresses are truncated at 124 characters in this message. TARGET LIST displays the entire host address value.

System action: The TARGET command ends in error.

Operator response: Correct and reissue the command. The TARGET NODE(*) LIST command may be issued to view information for each of the nodes, including their protocols and identifiers.

Destination: Descriptor code is 6.

Explanation: Volume specification and the specification of SMS information is not permitted on
the same TARGET command. The current volume specification or SMS information for node node-name is not altered. If SYSNAME information is present in this message, the node node-name is a multisystem node.

System action: The TARGET command ends in error.

Operator response: Issue the TARGET NODE(node-name) LIST command to view information for node node-name, including its volume specification or SMS information. Correct and reissue the command. Specifying VOLUME() causes any existing SMS information to be deleted. Similarly, specification of any of STORCLAS/MGMTCLAS/DATACLAS causes any existing volume specification to be deleted.

Destination: Descriptor code is 6.

IRRM019I subsystem-name SUBSYSTEM TARGET COMMAND COULD NOT LOCATE VOLUME volume. UCBLOOK RETURN CODE IS return-code. UCBLOOK REASON CODE IS reason-code.

Explanation: The TARGET command’s attempt to locate a UCB for volume volume failed. No changes are made to the node’s volume specification or SMS information.

System action: The TARGET command ends in error.

Operator response: Consult z/OS MVS Programming: Authorized Assembler Services Reference SET-WTO for the UCBLOOK service return and reason codes to determine why volume volume could not be located and take the appropriate action. Reissue a corrected version of the command, if necessary.

Destination: Descriptor code is 6. Routing code is 2.

IRRM020I subsystem-name SUBSYSTEM PURGE OF NODE node-name [SYSNAME system-name] [INMSG | OUTMSG] FILE file-name ENDED IN ERROR.

Explanation: The TARGET command was unable to erase all records from the INMSG or OUTMSG workspace file of node node-name. If the named node is a multisystem node, the member system’s SYSNAME is displayed in the message.

System action: The TARGET command ends in error.

Operator response: Report the occurrence of the message to the system programmer.

System programmer response: The error reflects a nonzero return code from a VSAM operation against the named workspace file.

If the integrity of the file is suspect, it might be necessary to replace the file. This can be done by deleting the node, erasing or renaming suspect file file-name, and then redefining the node. Alternatively, you could delete the node, then redefine it with a changed prefix to arrive at file names which differ from those of the previous workspace data sets.

If the integrity of the file is not suspect, the TARGET NODE(node-name) LIST command may be issued to determine the number of records in the file and a reissuance of the failed TARGET command can be attempted, if appropriate.

Destination: Descriptor code is 6.

IRRM021I subsystem-name SUBSYSTEM PURGE OF NODE node-name (SYSNAME sysname) [INMSG | OUTMSG] FILE file-name IS COMPLETE.

Explanation: The TARGET command has erased all records from the named file. If SYSNAME information is present in this message, the node node-name is a multisystem node.

Note: Commands pending to the file before its purge are processed.

System action: The TARGET command ends successfully.

Operator response: None.

Destination: Descriptor code is 6.

IRRM022I RRSF NODE node-name [SYSNAME system-name] CANNOT BE DELETED BECAUSE IT IS IN THE state STATE.

Explanation: An RRSF node cannot be deleted before it has first been made dormant. The indicated node was not deleted. If SYSNAME information is present in this message, the node node-name is a multisystem node.

System action: The TARGET command ends in error.

Operator response: To view a summary of the nodes and their current states, issue the TARGET LIST command. To delete node node-name, issue the TARGET NODE(node-name) DORMANT command, and then issue the TARGET LIST command to verify that node node-name is in a dormant state. Then reissue the failed TARGET NODE(node-name) DELETE command.

Destination: Descriptor code is 6.

IRRM023I INTERNAL STATE TRANSITION ERROR DETECTED. RRSF NODE node-name [SYSNAME system-name] IS CURRENTLY IN THE state STATE.

Explanation: Processing of the OPERATIVE/DORMANT/DELETE keyword of the TARGET command could not be completed successfully. The indicated RRSF node is left in the indicated connection state. If SYSNAME information is present in this message, the node node-name is a multisystem node.

System action: The TARGET command ends in error.
Operator response: Report the occurrence of this message to the system programmer.

System programmer response: Gather appropriate diagnostic information and contact the IBM support center.

Destination: Descriptor code is 6.

IRRM024I subsystem-name SUBSYSTEM TARGET COMMAND HAS FOUND THAT NO [protocol-name] NODES ARE CURRENTLY DEFINED.

Explanation: No other information can be displayed in response to a TARGET LIST command because no nodes, or nodes with the specified protocol-name are defined.

System action: The TARGET command ends successfully.

Operator response: None.

Destination: Descriptor code is 6.

IRRM025I subsystem-name SUBSYSTEM TARGET COMMAND DOES NOT ALLOW THE FILESIZE KEYWORD TO BE SPECIFIED WITH A VALUE OF filesize.

Explanation: The allowable range of values that can be specified with the FILESIZE keyword is 1 and 2147483647 (2 gigabytes minus 1).

System action: The TARGET command ends in error.


Destination: Descriptor code is 6.

IRRM026I NODE(*) AND SYSNAME(*) SHOULD NOT BE SPECIFIED TOGETHER. SYSNAME WILL BE IGNORED.

Explanation: When NODE(*) is specified, the SYSNAME(*) keyword is not necessary and is ignored.

System action: SYSNAME(*) is ignored and a detailed LIST of every node and sysname definition is displayed.

Operator response: None.

Destination: Descriptor code is 6.

IRRM027I RRSF NODE node-name IS A MULTISYSTEM NODE AND THE TARGET COMMAND MUST BE SPECIFIED WITH A SYSNAME FOR ALL FUNCTIONS EXCEPT LIST.

Explanation: The SYSNAME() keyword is mandatory on all TARGET commands that refer to multisystem nodes, except for LIST. The SYSNAME() keyword was specified on a previous TARGET command for node node-name. When the keyword SYSNAME() is specified, the node is always considered a multisystem node.

System action: The TARGET command is not processed.

Operator response: Reissue the command with SYSNAME information or with SYSNAME(*) to display all the systems associated with the specified node.

Destination: Descriptor code is 6.

IRRM028I RRSF NODE node-name IS A SINGLE-SYSTEM NODE AND MAIN SHOULD NOT BE SPECIFIED.

Explanation: Keyword MAIN can only be specified when referring to TARGET definitions that describe multisystem nodes.

System action: The TARGET command ends in error.

Operator response: If the single-system node is to be changed to a multisystem node, the TARGET command must include the new SYSNAME and the node node-name must be in one of the dormant states. Correct and reissue the command.

Destination: Descriptor code is 6.

IRRM029I RRSF NODE node-name IS A SINGLE-SYSTEM NODE AND THE SYSNAME PARAMETER IS NOT ALLOWED.

Explanation: The keyword SYSNAME was specified on a TARGET command that refers to an already existing TARGET definition describing a single-system node. Because the node is already considered a single-system node, SYSNAME should not be specified.

System action: The TARGET command is ignored.

Operator response: If the APPC single-system node is to be changed to a multisystem node, the TARGET command must also include the keyword MAIN and the node node-name must be in one of the dormant states. Correct and reissue the command.

Note: TCP nodes cannot be converted from single-system to multisystem. The existing node must be deleted and then defined as a multisystem node.

Destination: Descriptor code is 6.

IRRM030I RRSF NODE node-name [SYSNAME system-name] MUST BE IN SOME FORM OF THE DORMANT OR INITIAL STATE TO REDEFINE A SINGLE-SYSTEM NODE AS A MULTISYSTEM NODE.
**Explanation:** The keywords SYSNAME and MAIN were specified on a TARGET command that refers to an already existing TARGET definition describing a single-system node. Because SYSNAME and MAIN were specified on the TARGET command, RACF assumes that the single-system node is being redefined to be a multiscystem node. This message is issued if either of the following conditions occurs:

- You are redefining a remote single-system node to be a multisystem node, and the node is not in either the dormant or initial state.
- You are redefining a local single-system node to be a multisystem node, and one of its remote nodes is in a state other than the dormant or initial state.

**System action:** The TARGET command is ignored.

**Operator response:** If the single-system node is to be changed to a multisystem node, node-name must be in the dormant or initial state. Reissue a corrected version of the command.

**Destination:** Descriptor code is 6.

---

**IRR031I** DEFINED RRSF NODE node-name SYSNAME system-name REQUIRES A PREFIX AND LUNAME TO CONFIGURE A NEW MAIN.

**Explanation:** A TARGET command with keyword MAIN was issued to reconfigure the local system as the new MAIN system. RACF must access the workspace data sets used by the old MAIN system. In this case, RACF has looked for the PREFIX and LUNAME value that was specified on the TARGET statement for NODE node-name SYSNAME system-name and determined that one or both are missing. Because RACF cannot access the old MAIN’s workspace data sets, the multisystem node is not reconfigured.

**System action:** The TARGET command ends in error and a new MAIN is not configured.

**Operator response:** Issue a TARGET command to supply node-name sysname system-name with the missing information. Next, reissue the TARGET command to configure a new MAIN.

**Destination:** Descriptor code is 6.

---

**IRR032I** subsystem-name SUBSYSTEM TARGET COMMAND DOES NOT ALLOW NODE(*) AND SYSNAME TO BE SPECIFIED TOGETHER.

**Explanation:** When specifying NODE(*) to perform the LIST function, a specific SYSNAME cannot be specified.

**System action:** The TARGET command is ignored.

**Operator response:** Reissue the correct version of the command, if necessary. You can enter NODE(*)

**Destination:** Descriptor code is 6.
IRRM035I  subsystem-name SUBSYSTEM TARGET COMMAND CANNOT MAKE NODE node-name SYSNAME system-name [DORMANT | OPERATIVE] BECAUSE ONLY THE DEFINED STATE IS ALLOWED.

Explanation: The keyword OPERATIVE or DORMANT was specified on the TARGET command and because of the current configuration, node node-name system system-name can only be in the DEFINED state. This message is written to the SYSLOG.

System action: The OPERATIVE or DORMANT keyword is ignored and the TARGET command continues processing the remaining keywords.

Operator response: None.

IRRM036I  subsystem-name SUBSYSTEM TARGET COMMAND CANNOT DELETE NODE node-name MAIN SYSTEM system-name BECAUSE OTHER SYSTEMS EXIST IN NODE node-name.

Explanation: The TARGET command has detected an attempt to delete the MAIN system system-name of multisystem node node-name before all non-MAIN systems of node node-name have been deleted. TARGET command requires that the MAIN system be the last system deleted from a remote multisystem node.

System action: The TARGET command ends in error and the TARGET definition for node node-name system system-name is not deleted.

Operator response: Issue the appropriate TARGET commands to delete all non-MAIN systems of the multisystem node first, then reissue the original TARGET command to delete the MAIN system.

Destination: Descriptor code is 6.

IRRM037I  subsystem-name SUBSYSTEM TARGET COMMAND CANNOT ALLOCATE WORKSPACE DATASETS FOR NODE node-name SYSNAME system-name.

Explanation: A TARGET command attempted to change the system of a multisystem node that is considered the MAIN system. When this message is issued, the TARGET command either did not attempt to allocate the [INMSG | OUTMSG] workspace files of node node-name system system-name or it received a failure while attempting to allocate.

System action: The TARGET command ends in error.

Operator response: If allocation was not attempted, associated messages indicate the information that is needed. See the operator responses in each case. After supplying the information needed through additional TARGET commands, reissue the original command. If no other TARGET messages exist, allocation was attempted and failed. Report this failure to the system programmer.

System programmer response: Gather appropriate diagnostic information for the failing DYNALLOC and contact the IBM support center.

Destination: Descriptor code is 6.

IRRM038I  RRFS NODE node-name [SYSNAME system-name] MUST BE IN THE DORMANT STATE TO CONFIGURE A NEW MAIN.

Explanation: While configuring a new MAIN system in a multisystem node, a TARGET command located a node definition that should have a status of DORMANT, but it is in either the DEFINED, INITIAL, or one of the OPERATIVE states.

System action: The TARGET command ends in error.

Operator response: Issue the appropriate TARGET commands to put the named node and system in the DORMANT state. Reissue the original command to configure a new MAIN system.

Destination: Descriptor code is 6.

IRRM039I  RRFS NODE node-name [SYSNAME system-name] MUST BE IN THE DEFINED OR DORMANT STATE TO CONFIGURE A NEW MAIN.

Explanation: While configuring a new MAIN system in a multisystem node, a TARGET command located a node definition that should have a status of DEFINED or DORMANT, but it is in the INITIAL or one of the OPERATIVE states.

System action: The TARGET command ends in error.

Operator response: Issue the appropriate TARGET commands to put the named node and system in the DORMANT state. Reissue the original command to configure a new MAIN system.

Destination: Descriptor code is 6.

IRRM040I  RRFS NODE node-name [SYSNAME system-name] MUST BE IN THE DEFINED STATE TO CONFIGURE A NEW MAIN.

Explanation: While configuring a new MAIN system in a multisystem node, a TARGET command located a node definition that should have a status of DEFINED, but it is in the INITIAL state or one of the OPERATIVE or DORMANT states.

Destination: Descriptor code is 6.
System action: The TARGET command ends in error.

Operator response: Issue the appropriate TARGET commands to put the named node and system in the DEFINED state. System definitions in a multisystem node might not be in the DEFINED state because a MAIN system for the multisystem node has not been defined. After issuing the appropriate TARGET commands, issue the original TARGET command to configure a new MAIN system.

Destination: Descriptor code is 6.

IRRM041I subsystem-name SUBSYSTEM TARGET COMMAND CANNOT DELETE THE LOCAL NODE node-name MAIN SYSTEM system-name BECAUSE REMOTE RRSF NODES EXIST.

Explanation: The local MAIN system cannot be deleted until all remote RRSF nodes are deleted.

System action: The TARGET command ends in error.

Operator response: Issue the appropriate TARGET commands to delete all remote RRSF nodes. Next, reissue the failed TARGET command.

Destination: Descriptor code is 6.

IRRM049I subsystem-name SUBSYSTEM REQUIRES SMS STORCLAS SPECIFICATION IN ORDER TO ALLOCATE THE [INMSG | OUTMSG] WORKSPACE FILE OF NODE node-name [SYSNAME system-name].

Explanation: An SMS allocation for a node’s workspace data sets cannot be made without a STORCLAS specification. The TARGET command has detected the absence of such a specification for node node-name and does not attempt to allocate the node’s workspace data sets. If SYSNAME information is present in this message, the node node-name is a multisystem node.

System action: The TARGET command ends in error.

Operator response: Issue TARGET commands to provide the missing information along with the OPERATIVE or DORMANT keyword, as appropriate.

Destination: Descriptor code is 6.

IRRM050I subsystem-name SUBSYSTEM REQUIRES VOLUME SPECIFICATION IN ORDER TO ALLOCATE THE [INMSG | OUTMSG] WORKSPACE FILE OF NODE node-name [SYSNAME system-name].

Explanation: The absence of SMS information implies that a non-SMS allocation should be made for a node’s workspace data sets. This, in turn, requires a volume specification. The TARGET command has detected the absence of such a specification for node node-name and does not attempt to allocate the node’s workspace data sets. If SYSNAME information is present in this message, the node node-name is a multisystem node.

System action: The TARGET command ends in error.

Operator response: Issue TARGET commands to provide the missing information along with the OPERATIVE or DORMANT keyword, as appropriate.

Destination: Descriptor code is 6.

IRRM051I THE [INMSG | OUTMSG] WORKSPACE DATA SET OF (subsystem-name) SUBSYSTEM IS NOT ALLOCATED FOR NODE (node-name). THE DATA SET CANNOT BE PURGED.

Explanation: The TARGET command was unable to erase all records from the indicated data set of node node-name because no data set is allocated. This could be because

• the data set information was never provided by the user, or
• the RACF remote sharing facility (RRSF) marked the data set in error and deallocated it.

System action: The TARGET command ends in error.

Operator response: If this message occurred because the data set information was never provided by the user, issue the TARGET NODE(node-name) DORMANT command and supply any missing
IRRM054I • IRRM080I

information. See message IRRM011I for an indication of
the missing information. Also, see **z/OS Security Server
RACF Command Language Reference** for information
about the TARGET command.

If this message occurred because the RACF remote
sharing facility (RRSF) marked the data set in error and
deallocated it, issue:

- The TARGET NODE(node-name) LIST command to
  find out if the data set is allocated by RRSF.
- The TARGET NODE(node-name) DORMANT
  command to cause RRSF to attempt to allocate
  the data set. Next, issue the TARGET NODE(node-name)
  PURGE (INMSG/OUTMSG) command to purge the
  requested data set.

If you receive additional error messages indicating that
the above commands did not work, use the standard
data management commands to correct and update the
data set.

**Destination:** Descriptor code is 6.

---

IRRM054I subsystem-name SUBSYSTEM WAS
UNABLE TO ALLOCATE OUTMSG
WORKSPACE FILE workspace-dataset-
name OF NODE node-name [SYSNAME
system-name] FOR DEFINING OLD
MAIN SYSNAME system-name.

**Explanation:** While configuring a new MAIN system
in a multisystem node, an error was encountered while
attempting to allocate a workspace data set previously
used by the old MAIN system of this local node,
node-name. Shared DASD and a shared VSAM catalog
are recommended for the RRSF workspace data sets
due to this operation and when they are not used, the
workspace data set must be manually copied from the
old MAIN system to this new MAIN system (using the
same workspace file name).

**System action:** The TARGET command ends in error.

**Operator response:** Manually copy the workspace
data set from the old MAIN system to this new MAIN
system (using the same workspace file name) so that
this operation can continue.

**Destination:** Descriptor code is 6.

---

IRRM055I subsystem-name SUBSYSTEM TARGET
COMMAND CANNOT CHANGE THE
WDSQUAL VALUE FOR NODE
node-name [SYSNAME system-name]
BECAUSE ITS WORKSPACE FILES
ARE ALREADY ALLOCATED.

**Explanation:** The TARGET command has detected that
one or more workspace data sets for node node-name
are currently allocated and does not update the
WDSQUAL of node node-name. A node's WDSQUAL is
used in the formation of workspace data set names and
is changeable until those data sets have been allocated,
which normally occurs during processing of a
DORMANT/OPERATIVE keyword. After the data sets
have been allocated, it cannot be changed. If SYSNAME
information is present in this message, the node
node-name is a multisystem node.

**System action:** The TARGET command ends in error.

**Operator response:** Issue the TARGET
NODE(node-name) LIST command to view information
for node node-name, including its WDSQUAL. If a
different WDSQUAL for node node-name is required,
delete the node and redefine it with the new
WDSQUAL. Note that a new WDSQUAL value causes
a new set of workspace data sets to be created for the
node when it is reactivated. See **z/OS Security Server
RACF Command Language Reference** for information
about the TARGET command and the disposition of
workspace data sets affected by DELETE keyword
processing.

**Destination:** Descriptor code is 6.

---

IRRM056I subsystem-name SUBSYSTEM TARGET
COMMAND SPECIFIED A WDSQUAL
FOR NODE node-name [SYSNAME
system-name] WHICH IS CURRENTLY
NOT DEFINED AS A LOCAL NODE.
THE VALUE IS ACCEPTED BUT WILL
NOT BE USED UNTIL THE NODE IS
DEFINED AS LOCAL.

**Explanation:** The TARGET command has detected that
a WDSQUAL was specified for a node that is not
defined as a local node. WDSQUAL is only used in the
formation of workspace data set names for nodes that
are defined as local. Specifying WDSQUAL for a
remote node causes the WDSQUAL to be ignored in
the creation of its workspace data set names unless the
node is defined as local in a subsequent TARGET
command.

**System action:** Processing continues.

**Destination:** Descriptor code is 6.

---

IRRM080I subsystem-name SUBSYSTEM TARGET
COMMAND ENCOUNTERED AN
ERROR. ABEND CODE IS
returncode-reasoncode.

**Explanation:** The TARGET command processed by the
subsystem-name subsystem ended abnormally, with the
given return and reason codes.

**Operator response:** Report the occurrence of this
message to the system programmer.

**System programmer response:** Gather appropriate
diagnostic information and contact the IBM support
center.

**Destination:** Descriptor code is 6.
<table>
<thead>
<tr>
<th>IRRM082I</th>
<th>subsystem-name SUBSYSTEM TARGET COMMAND IS ALREADY PROCESSING.</th>
</tr>
</thead>
</table>

**Explanation:** The issuance of a TARGET command to be processed by the `subsystem-name` subsystem before the completion of a concurrent TARGET command has been detected. The processing of concurrent TARGET commands is not allowed.

**System action:** The TARGET command is ignored.

**Operator response:** The TARGET command may be reissued after the processing TARGET command has signaled its completion with message IRRM002I or IRRM003I.

**Destination:** Descriptor code is 6.

<table>
<thead>
<tr>
<th>IRRM083I</th>
<th>ISSUER HAS INSUFFICIENT AUTHORITY TO KEYWORD keyword ON subsystem-name SUBSYSTEM TARGET COMMAND.</th>
</tr>
</thead>
</table>

**Explanation:** RACF OPERCMDS class profiles currently fail to authorize the command issuer to use the named keyword with the TARGET command when invoking its execution by the `subsystem-name` subsystem.

**System action:** The TARGET command is ignored.

**Operator response:** See your RACF security administrator to obtain the appropriate authority.

**Destination:** Descriptor code is 6.

<table>
<thead>
<tr>
<th>IRRM084I</th>
<th>THE keyword KEYWORD REQUIRES ADDITIONAL SPECIFICATION.</th>
</tr>
</thead>
</table>

**Explanation:** The `keyword` keyword requires the specification of 1 or more of its options.

**System action:** The TARGET command is ignored.

**Operator response:** Reissue a corrected version of the command, if necessary.

**Destination:** Descriptor code is 6.

<table>
<thead>
<tr>
<th>IRRM085I</th>
<th>NODE node-name [SYSNAME system-name] CANNOT BE PURGED BECAUSE IT IS NOT DORMANT.</th>
</tr>
</thead>
</table>

**Explanation:** A node's workspace data sets cannot be purged unless the node is dormant. The TARGET command has detected that node `node-name` is not dormant. If SYSNAME information is included in the message, node `node-name` is a multisystem node.

**System action:** The TARGET command is ignored.

<table>
<thead>
<tr>
<th>IRRM086I</th>
<th>subsystem-name SUBSYSTEM TARGET COMMAND REQUIRES THAT A NODE BE SPECIFIED.</th>
</tr>
</thead>
</table>

**Explanation:** The NODE() keyword must be specified on any TARGET command that has additional keywords. The TARGET command has detected the presence of one or more such keywords along with the absence of the NODE() keyword.

**System action:** The TARGET command is ignored.

**Operator response:** Reissue a corrected version of the command, if necessary.

**Destination:** Descriptor code is 6.

<table>
<thead>
<tr>
<th>IRRM087I</th>
<th>subsystem-name SUBSYSTEM TARGET COMMAND REQUIRES THAT A PROTOCOL BE SPECIFIED FOR NODE node-name [SYSNAME system-name] TO IDENTIFY THE INTENDED PROTOCOL INSTANCE.</th>
</tr>
</thead>
</table>

**Explanation:** There is more than one protocol defined for node `node-name`. Each protocol instance can be separately modified, therefore, you must qualify the command by protocol in order to identify which instance you want to modify.

If SYSNAME `system-name` information is present in this message, the node `node-name` is a multisystem node, and the information is displayed for system `system-name` of the named node.

**System action:** The TARGET command ends in error.

**Operator response:** Specify the protocol by using the PROTOCOL keyword. Only the protocol name must be specified. For example, if you want to modify the TCP protocol instance, and the command you originally issued was:

```
TARGET NODE(NODEX) DESCRIPTION('THIS IS NODE X')
```

then reissue the command as:

```
TARGET NODE(NODEX) PROTOCOL(TCP) DESCRIPTION('THIS IS NODE X')
```

The order of the keywords is not important.

**Destination:** Descriptor code is 6.
IRRMO88I • IRRMO90I

IRRMO88I  REMOTE NODE node-name [SYSNAME system-name] CANNOT BE SPECIFIED AS THE LOCAL NODE BECAUSE MORE THAN ONE PROTOCOL HAS ALREADY BEEN DEFINED FOR IT.

Explanation: There is more than one protocol defined for node node-name. While remote node definitions can contain different workspace data set information for each protocol, the local node can only contain a single set of workspace data set information. Because there is more than one protocol instance already defined for node node-name, RRSF cannot determine which workspace data set information you intend to keep. This message is issued even if no file attributes are specified for either or both of the protocols.

If SYSNAME system-name information is present in this message, the node node-name is a multisystem node, and the information is displayed for system system-name of the named node.

System action: The TARGET command ends in error.

Operator response: Using TARGET LIST, note that the file attributes that you want to keep. Then, delete the other protocol instance, specify LOCAL, and add the protocol instance back to the node.

Example 1: If you originally specified:

```
TARGET NODE(NODEX) SYSNAME(SYSX) PROTOCOL(APPC(LUNAME(LU01))) WORKSPACE(VOLUME(VOL01) FILESIZE(600))
TARGET NODE(NODEX) SYSNAME(SYSX) PROTOCOL(TCP(PORTNUM(12601))) WORKSPACE(VOLUME(VOL02) FILESIZE(1000)) LOCAL
```

and if you want to keep the workspace attributes you had associated with the TCP protocol, then issue:

```
TARGET NODE(NODEX) SYSNAME(SYSX) PROTOCOL(APPC(LUNAME(LU01))) WORKSPACE(VOLUME(VOL01) FILESIZE(600)) LOCAL
TARGET NODE(NODEX) SYSNAME(SYSX) PROTOCOL(TCP(PORTNUM(12601))) WORKSPACE(VOLUME(VOL02) FILESIZE(1000))
```

Example 2: If you originally specified:

```
TARGET NODE(NODEX) SYSNAME(SYSX) PROTOCOL(APPC(LUNAME(LU01))) WORKSPACE(VOLUME(VOL01) FILESIZE(600)) LOCAL
TARGET NODE(NODEX) SYSNAME(SYSX) PROTOCOL(TCP(PORTNUM(12601))) WORKSPACE(VOLUME(VOL02) FILESIZE(1000)) LOCAL
```

and if you want to keep the workspace attributes you had associated with the TCP protocol, then split the previous command into two commands:

```
TARGET NODE(NODEX) SYSNAME(SYSX) WORKSPACE(VOLUME(VOL02) FILESIZE(1000)) LOCAL
TARGET NODE(NODEX) SYSNAME(SYSX) PROTOCOL(TCP(PORTNUM(12601)))
```

Destination: Descriptor code is 6.

IRRMO90I  YOU MUST SPECIFY MAIN WHEN ADDING A SECOND PROTOCOL INSTANCE TO MAIN NODE node-name SYSNAME system-name.

Explanation: RACF requires the definition of the MAIN system to be consistent when defining a second protocol.

System action: The TARGET command ends in error.

Operator response: Reissue the command, adding the MAIN keyword.

Destination: Descriptor code is 6.

IRRMO91I  LOCAL NODE protocol LISTENER STATUS IS [ACTIVE | INACTIVE | INITIALIZING].

Explanation: This is an informational message only. The status of the listener process for the protocol protocol on the local node and system at the time of the invocation of the TARGET command is as given.

The definitions of the values for status are:

- ACTIVE: The listener has been established and new connections can be established with remote nodes.
- INACTIVE: The listener is not currently available and no new connections can be established with remote nodes.
- INITIALIZING: The listener is attempting to start but has experienced a condition that prevents it from completing. The condition might not be permanent, therefore, the listener periodically tries again until it is successful or is stopped by making the local node DORMANT.

Operator response: None.

Destination: Descriptor code is 6.
IRRM092I  subsystem-name SUBSYSTEM TARGET COMMAND CANNOT MAKE NODE node-name [SYSNAME system-name] (OPERATIVE | DORMANT) BECAUSE NO LOCAL TCP INFORMATION IS DEFINED.

Explanation: The state of node node-name is not changed because no TCP protocol information has been defined for the local node. If SYSNAME information is present in this message, the NODE node-name is about a multisystem node and SYSNAME system-name is a member system of that node.

Operator response: Issue TARGET commands to define TCP protocol information for the local node and make the local node operative. Then reissue the TARGET command for the remote node.

Destination: Descriptor code is 6.

IRRM093I  subsystem-name SUBSYSTEM TARGET COMMAND CANNOT MAKE THE protocol2 PROTOCOL OF NODE node-name [SYSNAME system-name] (OPERATIVE | DORMANT) BECAUSE THE protocol1 PROTOCOL IS IN THE INITIAL STATE.

Explanation: When two protocol instances exist for a remote node, RRSF queues new requests only to the workspace data sets of the first protocol defined. The first protocol defined is protocol1, but it is in the INITIAL state (indicated by “???” in the TARGET LIST output), therefore, no workspace data sets are allocated. RRSF refuses to make the second protocol instance (protocol2) OPERATIVE or DORMANT, because that results in lost updates, since they cannot be queued.

If SYSNAME information is present in this message, the NODE node-name is a multisystem node and SYSNAME system-name is a member system of that node.

Operator response: Make the protocol1 protocol instance DORMANT or OPERATIVE, or delete it before making the protocol2 protocol instance DORMANT or OPERATIVE.

Destination: Descriptor code is 6.

IRRM094I  subsystem-name SUBSYSTEM TARGET COMMAND CANNOT MAKE THE protocol-name PROTOCOL OF NODE node-name [SYSNAME system-name] (OPERATIVE | DORMANT) BECAUSE A PROTOCOL CONVERSION IS IN PROGRESS.

Explanation: Creation of a new protocol instance in the DORMANT or OPERATIVE state is not allowed while a protocol conversion is in progress. When the conversion is complete, message IRRC058I is displayed on the console.


If SYSNAME information is present in this message, the node node-name is a multisystem node and sysname system-name is a member system of that node.

Operator response: Monitor the console for the issuance of message IRRC058I, which is issued when the workspace data sets of the old protocol are empty. While you wait for IRRC058I, you can issue TARGET LIST commands to monitor the status of the old protocol workspace data sets. After IRRC058I is issued, make a new protocol instance dormant or operative.

Destination: Descriptor code is 6.

IRRM095I  subsystem-name SUBSYSTEM TARGET COMMAND DOES NOT ALLOW PROTOCOL TO BE SPECIFIED WITH PURGE FOR THE LOCAL NODE.

Explanation: The PROTOCOL keyword is mutually exclusive with the PURGE keyword for the local node. Note that there can be only one set of workspace data sets for the local node, and it is completely independent of whatever protocol instances might exist for the local node.

Operator response: Reissue the command without PROTOCOL if you want to purge the workspace data sets of the local node. If you want to add a protocol instance to the local node, use a separate TARGET command, issuing TARGET PURGE, then TARGET PROTOCOL.

Destination: Descriptor code is 6.

IRRM096I  subsystem-name SUBSYSTEM TARGET COMMAND CANNOT CONFIGURE A NEW MAIN AT THIS TIME FOR MULTISYSTEM NODE node-name.

Explanation: You are attempting to change the MAIN system of a multisystem node. Dynamic MAIN system reconfiguration is only supported when both the old and new MAIN systems use the APPC protocol. The TARGET command fails because you are in one of the following situations:

1. The old or new MAIN system uses the TCP protocol.
2. The old or new MAIN system has more than one protocol instance defined.
3. The old or new MAIN system has a protocol conversion in progress (that is, it is processing two sets of workspace data sets).

Operator response: For situation 1, reconfigure to an APPC system if possible. For situation 2, if the
non-OPERATIVE protocol instance is a TCP instance that serves no purpose, delete it. For situation 3 if the conversion is to APPC, then wait for the conversion to complete. Message IRRC058I signals completion of the conversion process.

If you want to convert the MAIN system to a TCP system, you must delete the multisystem node definition and define it again with the new main system. This must be done on all RRSF nodes and done during a period of low administrative activity in order that updates are not lost.

Destination: Descriptor code is 6.

IRRM097I subsystem-name SUBSYSTEM TARGET COMMAND CANNOT MAKE NODE node-name [SYSNAME system-name] OPERATIVE BECAUSE ITS HOST ADDRESS IS UNKNOWN.

Explanation: The node definition for node-name does not contain a host address specification so the TARGET command cannot establish a connection. If SYSNAME information is present in this message, the node node-name is a multisystem node and SYSNAME system-name is a member system of that node.

Operator response: Assign a host address to the remote node by using the TARGET command and attempt to make the node operative again.

Destination: Descriptor code is 6.

IRRN000I RACF APPC RECEIVE TRANSACTION PROGRAM STARTING FOR LU luname NODE node-name [SYSNAME system-name].

Explanation: This is an informational message that is written to the SYSLOG after the program that receives APPC messages completes its initialization. The program now notifies APPC that it is ready to handle any messages from the indicated node. If SYSNAME information is present in this message, the node node-name is a multisystem node.

IRRN001I RACF REMOTE SHARING TCP COMMUNICATOR TASK STARTING FOR NODE node-name [SYSNAME system-name] WITH HOST ADDRESS address.

Explanation: This is an informational message that is written to the SYSLOG after the program that communicates between TCP nodes has completed its initialization. If SYSNAME information is present in this message, the node node-name is a multisystem node.

Note: The TCP host address is truncated at 124 characters. TARGET LIST displays the entire host address value.

IRRN003I APPC RECEIVE TRANSACTION PROGRAM OPERATING UNDER USER ID userid GROUP group-name.

Explanation: This message is written to the SYSLOG after the program that receives APPC messages completes its initialization. The program now notifies APPC that it is ready to handle any messages from the indicated node. This is an informational message.

IRRN009I RACF APPC RECEIVE TRANSACTION PROGRAM COMPLETED FOR LU luname NODE node-name [SYSNAME system-name].

Explanation: This message is written to the SYSLOG after the program that receives APPC messages stops processing incoming messages. The program stops as a result of an operator request to make the node dormant or as the result of an operational error. Earlier messages might indicate the nature of the problem. If SYSNAME information is present in this message, the node node-name is a multisystem node.

System action: The indicated node cannot send new work into the local node until the local node is returned to operative active status. Work requests active in the RACF subsystem address space for the indicated node continue to run. Any output directed to the failing node is held in the named node's OUTMSG workspace data set.

Operator response: Review the console log for an indication of the original error.

IRRN010I RACF REMOTE SHARING TCP COMMUNICATOR TASK TERMINATING FOR NODE node-name [SYSNAME system-name] WITH HOST ADDRESS address.

Explanation: This message is written to the SYSLOG after the program that communicates between TCP nodes stops processing incoming messages. The program stops as a result of an operator request (to restart the node's connection, to make the node dormant, or to stop the RACF address space) or as the result of an operational error. Earlier messages might indicate the cause of the problem. If SYSNAME information is present in this message, the node node-name is a multisystem node.
node-name is a multisystem node.

Note: The TCP host address is truncated at 124 characters. TARGET LIST displays the entire host address value.

System action: The indicated node cannot send new work to the local node until the remote connection is returned to operative active status. Work requests active in the RACF subsystem address space for the indicated node continue to run. Any output directed to the failing node is held in the named node’s OUTMSG workspace data set.

Operator response: Review the console log for an indication of the original error.

IRR020I  APPC RECEIVE AND WAIT STARTING FOR LU luname NODE node-name [SYSNAME system-name].

Explanation: This message is written to the SYSLOG immediately before the program notifies APPC that it received messages for the named LU name. If SYSNAME information is present in this message, the node node-name is a multisystem node.

System action: RACF continues processing.

Problem Determination: Under normal circumstances, this message can be ignored. When diagnosing a problem with a particular node, this message can be used with its companion messages to identify the part of the process that is failing.

When the receive program starts, it issues messages IRRN000I and IRRN003I. You can use these messages to verify that the correct APPC conversation was established and that it is established under the correct authority.

After issuing the messages, the program reads the INMSG workspace data set for any work that did not complete before the node became inactive.

Following the recovery of the held work requests, message IRRN020I is issued and APPC is notified. If IRRN009I is displayed, there is a problem in passing the work requests onto the task that routes the work within the subsystem address space.

IRR081I subsystem-name RACF SUBSYSTEM APPC RECEIVE TRANSACTION PROGRAM ENCOUNTERED AN ERROR. ABEND CODE IS abend-code.

Explanation: Every RACF remote sharing system has an APPC receive program receiving messages from other nodes defined to RACF. The receive transaction program had an error. This message is displayed every time an abnormal event occurs. This message is written to the SYSLOG.

System action: The transaction program attempts to try again during its startup processing when it is starting work from the INMSG workspace data set. If an abend occurs during this processing, the program discards the record and reads the next record in the data set. When all records have been read, the subsystem notifies APPC that it is ready to receive new messages.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. For a complete discussion, see z/OS Security Server RACF Diagnosis Guide.

Operator response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see z/OS MVS System Codes.

IRR081I subsystem-name RACF SUBSYSTEM APPC RECEIVE TRANSACTION PROGRAM ENCOUNTERED AN ERROR. ABEND CODE IS abend-code. RECEIVE TRANSACTION PROGRAM ENDING.

Explanation: Every RACF remote sharing system has an APPC receive program receiving messages from other nodes defined to RACF. The receive transaction program had an error.

System action: The transaction program cannot try again from this abnormal error. The program releases all system resources it holds and ends processing. The node connection program attempts to restart the receive transaction program.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. For a complete discussion, see z/OS.
Security Server RACF Diagnosis Guide

Operator response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see z/OS MVS System Codes.

Destination: Descriptor code is 6. Routing code is 2.

**RRSF connection send transaction program messages**

**IRRO080I**  
subsystem-name RACF SUBSYSTEM  
APPC SEND TRANSACTION  
PROGRAM ENCONTERED AN  
ERROR. ABEND CODE IS abend-code.

Explanation: Every RACF remote sharing system has an APPC send program sending messages to other nodes defined to RACF. The send transaction program had an error. This message appears every time an abnormal event occurs. This message is written to theSYSLOG.

System action: The transaction program attempts to try the current transaction again.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. For a complete discussion, see Security Server RACF Diagnosis Guide.

Operator response: Report the occurrence of the message to the system programmer.

Problem Determination: If the abend code is ???-??, then no SDWA was provided and RACF could not determine the abend code.

For an explanation of these codes, see z/OS MVS System Codes.

Destination: Descriptor code is 6. Routing code is 2.

**IRRO081I**  
subsystem-name RACF SUBSYSTEM  
APPC SEND TRANSACTION  
PROGRAM ENCONTERED AN  
ERROR. ABEND CODE IS abend-code.  
SEND TRANSACTION PROGRAM ENDING.

Explanation: Every RACF remote sharing system has an APPC send program sending messages to other nodes defined to RACF. The send transaction program had an error. This message is displayed every time an abnormal event occurs.

System action: The transaction program cannot retry from this abnormal error. The program releases all system resources it holds and ends processing. The node connection program attempts to restart the send transaction program.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. For a complete discussion, see Security Server RACF Diagnosis Guide.

Operator response: Report the occurrence of the message to the system programmer.

Problem Determination: If the abend code is ???-??, then no SDWA was provided and RACF could not determine the abend code.

For an explanation of these codes, see z/OS MVS System Codes.

Destination: Descriptor code is 6. Routing code is 2.

**RRSF (RACF remote sharing facility) general messages**

**IRRP003I**  
subsystem-name SUBSYSTEM WAS UNABLE TO ISSUE IEFSSREQ REQUEST. RETURN CODE IS: return-code.

Explanation: An attempt to send a request to the MVS IEFSSREQ subsystem has failed. Profiles have been updated on the source-node.

System action: IEFSSREQ request processing ends.

Operator response: Report this message to your system programmer.

System programmer response: The return code indicated in this message reflects the return code from the MVS IEFSSREQ subsystem interface. The return code might be one of these values:

<table>
<thead>
<tr>
<th>Return Code</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>The subsystem does not support this function.</td>
</tr>
<tr>
<td>8</td>
<td>The subsystem exists, but is not active.</td>
</tr>
<tr>
<td>12</td>
<td>The subsystem is not defined in the IEFSSNxx parmlib member.</td>
</tr>
<tr>
<td>16</td>
<td>The function has not completed. This is a disastrous error.</td>
</tr>
<tr>
<td>20</td>
<td>The SSOB or SSIB have invalid lengths or formats.</td>
</tr>
<tr>
<td>24</td>
<td>The SSI has not been initialized.</td>
</tr>
</tbody>
</table>
A return code of 4, 16, 20, or 24 indicates a RACF code problem. Report this message to the IBM support center.

A return code of 8 or 12 indicates an installation or RACF subsystem configuration problem. See z/OS Migration for installation considerations and z/OS Security Server RACF System Programmer’s Guide for configuration considerations for the RACF subsystem.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.

---

**IRR004I**  
**subsystem-name SUBSYSTEM IEFSSREQ REQUEST ENDED WITH A RETURN CODE OF return-code.**

**Explanation:** An attempt to send a request to the MVS IEFSSREQ subsystem interface failed. No profiles have been updated.

**System action:** RACLINK command processing ends.

**Operator response:** Report this message to your system programmer.

**System programmer response:** The return code indicated in this message is the value of the SSOBRETN field in the subsystem’s option block (SSOB). The return code might be one of these values:

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>The subsystem could not execute the command because of an internal parameter error, or the subsystem supports this request, but is not active.</td>
</tr>
<tr>
<td>16</td>
<td>The caller is not APF-authorized, or storage is unavailable for an internal data area.</td>
</tr>
</tbody>
</table>

Contact the IBM support center to report this problem.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.

---

**IRR016I**  
**Undefined association (node-name.userid) could not be [deleted | retrieved] by userid userid at node node-name.**

**Explanation:** The RACLINK APPROVE or RACLINK UNDEFINE command failed because the user ID association does not exist on the target side. The user ID association has been updated on the source user ID, but not on the target user ID. This message is sent to the TSO terminal of the RACLINK issuer or the target user.

**System action:** RACLINK command ends processing.

**User response:** If you issued the failing RACLINK APPROVE command, you need to use the RACLINK UNDEFINE(node-name.userid) command to delete any indicators of a user ID association between you and node-name.userid. Then use the RACLINK DEFINE(node-name.userid/password) command or both RACLINK DEFINE(node-name.userid) command on this node and RACLINK APPROVE command on node node-name to complete the definition of the user ID association.

**RACF Security Administrator Response:** Analyze the supplied return code by reading the return code description for the ICHEINTY macro in z/OS Security Server RACF Macros and Interfaces. Contact the IBM support center, if necessary.

**Destination:** Descriptor code is 6. Routing code is 9.
**IRRP017I** The requested association could not be defined | approved | deleted | retrieved | updated because user userid is not RACF defined.

**Explanation:** The association specified on the RACLINK LIST, DEFINE, APPROVE, or UNDEFINE command could not be located because the target user ID is not defined to RACF. The source user ID might have been updated. This message is sent to the TSO terminal of the RACLINK issuer or the target user.

**System action:** RACLINK command processing completes.

**User response:** Either add the target user ID by way of the ADDUSER command or contact your RACF administrator to do so. After the problem has been corrected, try the command again.

**IRRP018I** An existing association was found for user userid on target node node-name.

**Explanation:** A RAclink DEFINE was issued for an association that exists on the target node. The source user ID was updated, but the target user ID was not. This message is sent to the TSO terminal of the RACLINK issuer.

**System action:** RACLINK command processing completes.

**User response:** Issue the RAclink DELETE command to delete the existing association and then try the command again.

**IRRP019I** Association key length length is not valid. Information cannot be retrieved for user userid.

**Explanation:** A RAclink command has failed because the user ID and node are too long. This error is due to an internal problem. This message is sent to the TSO terminal of the RAclink issuer.

**System action:** RACLINK command processing ends. No RACLINK association is retrieved.

**User response:** Contact IBM support to correct the faulty key length.

**IRRP020I** RACF ICHEINTY rc return-code received while defining | approving | deleting | retrieving | updating association (node-name.userid) for user userid.

**Explanation:** The RAclink command failed while attempting to define, approve, delete, retrieve, or update the association information for the specified user ID. This might have occurred on the local node or a different node. This message is sent to the TSO terminal of the RAclink issuer or the target user.

**System action:** RAclink command ends processing.

No RAclink association is retrieved.

**User response:** Contact your system programmer to analyze the supplied return codes.

**System programmer response:** To determine the meaning of these ICHEINTY return codes, see z/OS Security Server RACF Macros and Interfaces.

**IRRP021I** RAclink could not be completed because target node node-name is undefined.

**Explanation:** RACF is unable to locate the node name specified. This message is sent to the TSO terminal of the target user.

**System action:** RAclink command ends processing. A RAclink association on the source user ID might have been updated.

**User response:** Verify that this is a legitimate node to be sending commands to and, if it is, contact your system programmer to have the remote node defined to RACF.

**System programmer response:** Issue the TARGET LIST command to determine the status of the target node. Use the TARGET command if the node must be defined.

**IRRP022I** RAclink command was unable to obtain storage for the association entry.

**Explanation:** A failure occurred while attempting to obtain storage necessary to update an association entry in the target user’s profile. This message is sent to the TSO terminal of the RAclink issuer.

**System action:** RAclink command processing ends. The local user profile has been updated, but the target user profile has not been updated.

**User response:** Notify the system programmer. Once the storage problem has been resolved, delete the association from the local user profile and issue the failing RAclink command again.

**System programmer response:** Note the message number and any other diagnostic information generated, and contact your IBM support center.

**Problem Determination:** The storage request was for subpool 1.

**IRRP080I** subsystem-name SUBSYSTEM MESSAGE TASK HAS ENCOUNTERED AN ERROR. ABEND CODE IS abend-code.

**Explanation:** The MESSAGE handler task was processing a command or returned output. This message appears when an abnormal event occurs.

**System action:** The MESSAGE handler attempts to retry the current work request. If the retry does not
work, message IRRP081I is issued.

**Operator response:** Report the occurrence of the message to the system programmer.

**Problem Determination:** For an explanation of these codes, see [z/OS MVS System Codes](#).  

**Destination:** Descriptor code is 1. Routing codes are 2 and 9.

---

**IRRP081I**  
**subsystem-name** SUBSYSTEM MESSAGE  
**TASK HAS ENCLOSED AN ERROR. ABEND CODE IS abend-code.**  
**MESSAGE HANDLING TASK ENDING.**

**Explanation:** The message handler subtask was processing a command or returned output. This message appears when an abnormal event occurs.

**System action:** The message handler subtask ends and the parent process attempts to restart the message handler subtask.

**Operator response:** Report the occurrence of the message to the system programmer.

**Problem Determination:** For an explanation of these codes, see [z/OS MVS System Codes](#). The task that started the message handler task attempts to restart the task. Verify that message IRRB020I was issued showing that the task restart was successful.

**Destination:** Descriptor code is 6. Routing code is 2.

---

**IRRP092I**  
**(Peer | Managed) association with userid at node node-name established for you by userid.**

**Explanation:** An association with target-userid has been established for you by userid. This message is sent to the TSO terminal of the target user.

**System action:** The RACLINK command completes successfully.

**User response:** None.

---

**IRRP093I**  
**(Peer | Managed) association with userid at node node-name issued by command-issuer waiting for your approval.**

**Explanation:** A RACLINX DEFINE specifying you as the target user ID was issued by the command-issuer. The association is not active until you approve it. This message is sent to the TSO terminal of the target user.

**System action:** The RACLINK command has completed processing. The association is pending approval.

**User response:** If the association is wanted, approve the association with the RACLINK APPROVE command.

---

**IRRP095I**  
**(Peer | Managed) association with userid1 at node node-name by userid2 failed because user access has been revoked.**

**Explanation:** The indicated association for userid2 could not be defined because userid1’s access has been revoked. This message is sent to the TSO terminal of the RACLINK issuer.

**System action:** The RACLINK command stops processing.

**User response:** Contact your RACF security administrator to find out why userid1 has been revoked, and to possibly have it resumed.

---

**IRRP096I**  
**(Peer | Managed) association with userid at node node-name by command-issuer failed. RACROUTE VERIFY RACF rc is return-code.**

**Explanation:** A RACLINT DEFINE command was issued and the validity checking for the remote user ID failed. This message is sent to the TSO terminal of the RACLINK issuer.

**System action:** The RACLINK command stops processing.

**User response:** To determine the exact cause of the failure, see the information about RACROUTE REQUEST=VERIFY in [z/OS Security Server RACROUTE Macro Reference](#).

---

**IRRP097I**  
**(Peer | Managed) association with userid at node node-name has been approved.**

**Explanation:** The indicated association has been approved. Remote sharing requests to the target user ID are processed. This message is sent to the TSO terminal of the RACLINK issuer or the target user.
System action: The RACLINK command completes processing.
User response: None.

Explanation: The specified association has been deleted from your user ID profile by the specified user ID. This message is sent to the TSO terminal of the target user.

System action: The RACLINK command completes processing.
User response: None.

Explanation: Either a RACLINK DEFINE or a RACLINK APPROVE command was issued specifying your user ID as the target of the command. However, this user ID association is already created and approved in your user ID profile. No update has been made to your user ID profile. This message is sent to the TSO terminal of the target user.

System action: The RACLINK command ends.
User response: None.

Explanation: The RACLINK entry could not be defined because of a mismatch. This could have occurred because:

- The association exists in your user ID profile, but the association is waiting for approval from userid.
- The association exists in your user ID profile, but the association type is different. For example, the existing association is of type PEER and an attempt was made to create an association of type MANAGED.

This message is sent to the TSO terminal of the target user.

System action: The RACLINK command ends processing. A pending association has been created in the source user ID profile, and the association in the target user ID profile remains unchanged.

User response: If the association must be modified, delete it using the UNDEFINE operand of the RACLINK command. Follow this by issuing a RACLINK DEFINE command.

Problem Determination: For information about the pending association waiting for your approval, use the RACLINK LIST command.
RRSF connection task messages

IRRQ001I RACF REMOTE SHARING TCP CONNECTOR TASK STARTING FOR NODE node-name [SYSNAME system-name] WITH HOST ADDRESS address.

Explanation: This is an informational message that is written to the SYSLOG after the program that establishes a connection to a remote TCP node has completed its initialization. The connector task is started by the local listener task when a request is made to establish an operative connection with a remote node.

Note: The TCP host address truncates at 124 characters. TARGET LIST displays the entire host address value.

IRRQ010I RACF REMOTE SHARING TCP CONNECTOR TASK TERMINATING FOR NODE node-name [SYSNAME system-name] WITH HOST ADDRESS address.

Explanation: This message is written to the SYSLOG as the program that establishes a connection to a remote TCP node stops processing. The program stops normally when the outbound connection request is successful. The program can also stop as the result of an internal error (ABEND). Earlier messages might indicate the nature of the problem.

IRRQ015I task-name TASK IN subsystem-name SUBSYSTEM HAS ENDED ABNORMALLY.

Explanation: During the shutdown process, the task task-name in the subsystem subsystem-name would not voluntarily shut down. The CONNECTION program has waited a sufficient interval for the task to end, without success. The task is forcibly ended. This message is written to the SYSLOG.

System action: Task task-name is ended abnormally. The CONNECTION program continues the shutdown process.

Operator response: Report the exact text of this message to your system programmer.

System programmer response: Examine any system dumps obtained.

IRRQ811I subsystem-name SUBSYSTEM APPC CONNECTION TASK HAS ENCOUNTERED AN ERROR. ABEND CODE IS abend-code. CONNECTION TASK ENDING.

Explanation: The CONNECTION task was changing the status of an APPC conversation and the related transaction programs because of a TARGET command request. This message is displayed when an abnormal event occurs during a task you cannot try again.

System action: The CONNECTION task releases system resources it holds and ends processing.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. For a complete discussion, see z/OS Security Server RACF Diagnosis Guide.

Operator response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see z/OS MVS System Codes.

IRRQ180I subsystem-name SUBSYSTEM protocol-name task-name TASK HAS ENCOUNTERED AN ERROR. ABEND CODE IS abend-code.

Explanation: The remote sharing task-name task for the protocol-name protocol experienced an abnormal error. This message is written to the SYSLOG.

System action: The task attempts to continue.

Destination: Descriptor code is 6. Routing code is 2.
When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. For more information, see z/OS Security Server RACF Diagnosis Guide.

Operator response: Report the occurrence of the message to the system programmer.

Problem Determination: For an explanation of these codes, see z/OS MVS System Codes. The task that started the task-name task attempts to restart the task.

Destination: Descriptor code is 6. Routing code is 2.

For the TCP protocol, the following values for task-name might appear (for messages IRRQ180I and IRRQ181I):

<table>
<thead>
<tr>
<th>Task name</th>
<th>Module name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISTENER</td>
<td>IRRTCP00</td>
<td>Listens for connection requests initiated by remote nodes, and manages the subsequent subtasks.</td>
</tr>
<tr>
<td>CONNECTOR</td>
<td>IRRTCP01</td>
<td>Establishes a connection with a given remote node.</td>
</tr>
<tr>
<td>COMMUNICATOR</td>
<td>IRRTCP02</td>
<td>Sends and receives remote sharing requests for a given remote node.</td>
</tr>
</tbody>
</table>

**Table 1. TCP protocol task-name values**

RRSF output handling task messages

**IRR0001I**  RACF command output transmitted because user data set data-set-name is full.

Explanation: Output was returned from one of the following to the issuer by way of TSO TRANSMIT because the output data set of the user is full:

- A directed command
- An automatically directed command
- An automatically directed password
- A password synchronization request
- An automatically directed application update

This message is sent to the TSO terminal of the user.

System action: None.

User response: Allocate a larger data set or delete lines from the existing data set.

**IRR002I**  RACF command output transmitted because user data set data-set-name could not be allocated. Allocation return code was return-code.

Explanation: Output was returned from one of the following to the issuer by way of TSO TRANSMIT because allocation of the output data set of the user failed with the indicated return code:

- A directed command
- An automatically directed command
- An automatically directed password
- A password synchronization request
- An automatically directed application update

During returned output processing, RACF performs dynamic allocation for the RRSFLIST data set. If this fails, RACF returns the return code. This message is sent to the TSO terminal of the user.
System action: None.
User response: Report the complete text of this message to the system programmer.

System programmer response: The MVS service that gave the indicated return code is DYNALLOC. To determine the meaning of the return code, see z/OS MVS Programming: Authorized Assembler Services Guide. Look up the section on dynamic allocation return and reason codes. Dynamic allocation is also known as SVC 99, and may be documented that way. If the problem persists, gather appropriate diagnostic information and contact the IBM support center.

IRRR003I RACF command output transmitted because user data set data-set-name format is not correct.

Explanation: Output was returned from one of the following to the issuer by way of TSO TRANSMIT because the output data set of the user does not have the required format:
- A directed command
- An automatically directed command
- An automatically directed password
- A password synchronization request
- An automatically directed application update

Output data sets must have DSORG=PS, LRECL=80. This message is sent to the TSO terminal of the user.

System action: None.
User response: If you want directed command output to be written to a data set, replace your erroneous x.x.x.x.x.RRSFLIST data set with one that has the required DSORG and LRECL.

IRRR004I RACF command output transmitted because user data set data-set-name could not be opened. Abend code is abend-code.

Explanation: Output was returned from one of the following to the issuer by way of TSO TRANSMIT:
- A directed command
- An automatically directed command
- An automatically directed password
- A password synchronization request
- An automatically directed application update

Allocation of the output data set of the user failed because the output data set could not be opened for write access.

System action: None.
User response: If you have authorization to the data set, report the complete text of this message to the system programmer. If you do not have authorization to the data set, contact the RACF security administrator to address the problem of authorization. You will continue to receive returned output by way of TSO TRANSMIT as long as you cannot open the data set.

System programmer response: Gather appropriate diagnostic information and contact the IBM support center.

IRRR005I The initial portion of the command output is unavailable.

Explanation: The first portion of the returned output from a directed RACF command was lost. This message is appended to the RRSFLIST data set of the user. If the data set is full, this message is transmitted to the TSO terminal of the user.

System action: None.
User response: Report the complete text of this message to the system programmer or RACF security administrator.

System programmer response: One or more records containing the returned output from the command could not be located within the appropriate INMSG workspace file. Gather appropriate diagnostic information and contact the IBM support center.

IRRR006I Command output was truncated at this point.

Explanation: A portion of the returned output from a directed RACF command was lost. This message marks the end of output that was retained. This message is appended to the RRSFLIST data set of the user. If the data set is full, this message is transmitted to the user’s TSO terminal.

System action: None.
User response: Report the complete text of this message to your system programmer or RACF security administrator.

System programmer response: One or more records containing the returned output from the command could not be located within the appropriate INMSG workspace file. Gather appropriate diagnostic information and contact the IBM support center.

IRRR007I Command output was resumed at this point.

Explanation: A portion of the returned output from a directed RACF command was lost. This message marks the beginning of output that was retained. This message is appended to the RRSFLIST data set of the user. If the data set is full, this message is transmitted to the TSO terminal of the user.

System action: None.
IRRR008I Command succeeded. There are no messages.

Explanation: The directed RACF command processed successfully at the execution node and generated no output. This message is appended to the RRSFLIST data set of the user. If the data set is full, this message is transmitted to the TSO terminal of the user.

System action: None.

User response: None.

IRRR009I Command ended with return code return-code. There are no messages.

Explanation: There was no output from a directed RACF command that failed at the execution node. This message is appended to the RRSFLIST data set of the user. If the data set is full, this message is transmitted to the TSO terminal of the user.

System action: None.

User response: If you suspect that the command failed because of user error, consider reissuing the RACF command. Otherwise, report the complete text of this message to your system programmer or RACF security administrator.

IRRR010I Command was not executed. Processing code code was returned by the executing node.

Explanation: A directed RACF command could not be processed because of an error at the execution node. This message is appended to the RRSFLIST data set of the user. If the data set is full, this message is transmitted to the TSO terminal of the user.

System action: None.

User response: If this message indicates a code other than 507, report the complete text of this message to your system programmer or RACF security administrator. If this message indicates a code of 507, try the command again.

Code Function
500 Internal error while trying to execute the command.
507 Task being restarted concurrently.
508 Error while parsing the command.
509 Command not a supported RACF command.
510 Command not supported with the sysplex ROUTE command.
511 Failure in the TSO IKJSCAN service.

Destination: Port the processing code from this message to the IBM service center.

IRRR011I command was successful at node node-name. Output [written to data-set-name | was sent via TSO TRANSMIT | was lost | was not requested]

Explanation: The output from a directed or automatically directed RACF command was received from the execution node. The output was returned to the user in the described manner or cannot be returned to the user because of error. If the output was “not requested”, the command was automatically directed, the SET AUTODIRECT OUTPUT setting for this user was NOOUTPUT, and the SET AUTODIRECT NOTIFY setting was ALWAYS, WARN, or FAIL. If the output was “lost”, an error occurred while attempting to return the output to the user, such as a workspace data set was damaged or a TRANSMIT was attempted to an incorrect node (as specified in the SET JESNODE command). This message is sent to the TSO terminal of the user.

System action: None.

User response: Examine your RRSFLIST data set or invoke TSO RECEIVE to view the returned output from the directed command. If the command output could not be returned, a TSO TRANSMIT attempt failed and you should contact your system programmer to report the failure.

IRRR012I command was unsuccessful at node node-name. Output [written to data-set-name | was sent via TSO TRANSMIT | was lost | was not requested]

Explanation: The output from a directed or automatically directed RACF command was received from the execution node. The output was returned to the user in the described manner or cannot be returned to the user because of error. If the output was “not requested”, the command was automatically directed, the SET AUTODIRECT OUTPUT setting for this user was NOOUTPUT, and the SET AUTODIRECT NOTIFY setting was ALWAYS, WARN, or FAIL. If the output was “lost”, an error occurred while attempting to return the output to the user, such as a workspace data set was damaged or a TRANSMIT was attempted to an incorrect node (as specified in the SET JESNODE command). This message is sent to the TSO terminal of the user.

System action: None.

User response: Examine your RRSFLIST data set or invoke TSO RECEIVE to view the returned output from the directed command. If the command output could not be returned, a TSO TRANSMIT attempt failed and you should contact your system programmer to report the failure.
Chapter 6. IRR messages for commands, utilities, and other tasks
was NOOUTPUT, and the SET AUTODIRECT NOTIFY setting was ALWAYS, WARN, or FAIL. If the output was “lost”, an error occurred while attempting to return the output to the user, such as a workspace data set was damaged or a TRANSMIT was attempted to an incorrect node (as specified in the SET JESNODE command). This message is displayed by way of TSO SEND to the user's terminal.

User response: If the command output was returned, check its contents for additional error messages, such as error message IRRR016I. Additional error messages may have been sent to the operator console or records written to SYS1.LOGREC.

**IRRR018I** command not processed at node node-name. Output was sent via TSO TRANSMIT | was lost | was not requested

Explanation: This message is sent to a user through the TSO SEND command. It is notification of the results of a directed or automatically directed command. The command was sent to a target node, but an error occurred before or during the processing of the command on that node. For example, the target user ID may not exist or is revoked. If the output was “not requested”, the command was automatically directed, the SET AUTODIRECT OUTPUT setting for this user was NOOUTPUT, and the SET AUTODIRECT NOTIFY setting was ALWAYS, WARN, or FAIL. If the output was “lost”, an error occurred while attempting to return the output to the user, such as a workspace data set was damaged or a TRANSMIT was attempted to an incorrect node (as specified in the SET JESNODE command). This message is displayed by way of TSO SEND to the terminal of the user.

User response: If the command output was returned, check its contents for additional error messages, such as error message IRRR016I. Additional error messages may have been sent to the operator console or records written to SYS1.LOGREC.

**IRRR019I** unable to establish RACF environment to process output received from node node-name.

Explanation: The RACF subsystem address space attempted to send command output or results from one of the following on the indicated node to a user on the local node.

- A directed command
- An automatically directed command
- An automatically directed password
- A password synchronization request
- An automatically directed application update

When establishing the RACF environment for the user, the RACROUTE REQUEST=VERIFY failed, possibly because the user does not exist. This message is accompanied by message IRRR011I, which names the user ID and contains the RACROUTE REQUEST=VERIFY return codes.

System action: The command output or results are not returned to the intended user.

User response: Determine why the RACROUTE REQUEST=VERIFY failed, based on the return and reason codes in accompanying message IRRR011I.

If the user ID does not exist (RACROUTE return code is 4 and RACF return code is 4 in message IRRR011I), an incorrect user ID was specified on the SET command on the indicated node. Issue the SET LIST command on the indicated node to display the current OUTPUT and NOTIFY settings for automatic command direction. Note where the incorrect user ID appears and issue the SET command with the appropriate OUTPUT and NOTIFY keywords to correct the error.

If there is some other problem with the user ID (the return codes are different than stated above), report the exact text of this message and accompanying message IRRR011I to your RACF security administrator.

RACF Security Administrator Response: The return and reason codes from RACROUTE REQUEST=VERIFY are documented in z/OS Security Server RACROUTE Macro Reference. Based on what the codes indicate (for example, the user ID is revoked), correct the error appropriately (for example, resume the user ID).

Destination: Descriptor code is 4. Routing codes are 2 and 9.

**IRRR020I** password synchronization unsuccessful at node node-name. Output was sent via TSO TRANSMIT.

Explanation: RACF has encountered an error during the processing of a password synchronization request. Output from the password synchronization request has been sent by way of the TSO TRANSMIT command or written to your RRSFLIST data set. This message is displayed by way of TSO SEND to the terminal of the user.

System action: The system continues processing.

User response: Examine the output from the password synchronization request to determine the nature of the error.

**IRRR021I** password synchronization successful at node node-name.

Explanation: RACF has successfully processed a password synchronization request at the node specified.
in the message. Output from the password synchronization request has been written to your RRSFLIST data set. This message is displayed by way of TSO SEND to the terminal of the user. This is an informational message.

**System action:** The system continues processing.

---

**IRR080I** subsystem-name SUBSYSTEM OUTPUT HANDLING TASK HAS ENCOUNTERED AN ERROR. ABEND CODE IS returncode-reasoncode.

**Explanation:** In attempting to return the output from a directed RACF request, a task within the subsystem-name subsystem ended abnormally, with the given return and reason codes.

**Operator response:** Report the occurrence of the message to the system programmer.

**System programmer response:** Gather appropriate diagnostic information and contact the IBM support center.

**Destination:** Descriptor code is 6. Routing code is 2.

---

**IRR101I** Application update request completed successfully for class class-name, profile name profile-name.

**Explanation:** Profile profile-name in class class-name has been updated successfully.

**System action:** The RACF database has been changed on both the source node and on the target node.

**User response:** The RACF database has been changed on both the source node and on the target node.

---

**IRR102I** request-type request unsuccessful, return code return-code, reason code reason-code, for class class-name, profile name profile-name.

**Explanation:** Profile profile-name in class class-name has not been updated, or was not completely updated. The request-type is ICHEINTY, RACDEF, or RACXTRT, depending on the request that was propagated. The failing request's return code is return-code and the reason code is reason-code. The return code and reason code are hexadecimal values.

**System action:** The RACF database is changed on the source node, but it is not changed, or is not completely changed, on the target node.

**User response:** Check the RRSFLIST output for additional information, such as the node where the failure occurred, the type of request, and, for ICHEINTY requests, additional ICH51nnn messages. The failing request's parameter list is also dumped with message IRRR105I. For RACDEF and RACXTRT requests, the parameter list being dumped is the RACROUTE parameter list generated by RRSF to transport the request to the target node.

**System programmer response:** For an explanation of the abend code, see z/OS MVS System Codes.

---

**IRR103I** RACROUTE request unsuccessful, RACROUTE return code racroute-return-code, RACF return code racf-return-code, RACF reason code racf-reason-code, for class class-name, profile name profile-name.

**Explanation:** Profile profile-name in class class-name was not updated, or has not been completely updated. The failing RACROUTE return code is racroute-return-code, the RACF return code is racf-return-code, and the RACF reason code is racf-reason-code. The return codes and reason code are hexadecimal values.

**System action:** The RACF database is changed on the source node, but it is not changed, or is not completely changed, on the target node.

**User response:** Check the RRSFLIST output for additional information, such as the node where the failure occurred, and the type of RACROUTE request. It is also possible that the databases are not synchronized. You can determine this by comparing a list of profiles on each system. The failing RACROUTE parameter list is also dumped with message IRRR105I.

---

**IRR104I** abend-code[yyy] abend during request-type processing for class class-name, profile name profile-name.

**Explanation:** An abend occurred while processing an application update for profile profile-name in class class-name. The request-type is ICHEINTY, RACROUTE, RACDEF, or RACXTRT, depending on the request that was propagated. The failing request abended with a system or user abend as indicated by the abend-code, for example S0C4. If a reason code was specified with the abend code, it is displayed as yyy.

**System action:** The RACF database was changed on the source node, but it might or might not have been changed on the target node.

**User response:** Check the RRSFLIST output for additional information, such as the node where the failure occurred. The failing request's parameter list is also dumped with message IRRR105I. For RACDEF and RACXTRT requests, the parameter list being dumped is the RACROUTE parameter list generated by RRSF to transport the request to the target node. A dump might have been produced on the node where the failure occurred. Notify the system programmer for that node.

**System programmer response:** For an explanation of the abend code, see z/OS MVS System Codes.
IRRR105I  Failing parameter list follows:

Explanation: An error occurred while performing an application update. This message is preceded by IRRR102I, IRRR103I, or IRRR104I, which provide additional information about the error. This message starts a display of a RACROUTE or ICHEINTY macro parameter list. If the error occurs for a RACXTRT or RACDEF, a RACROUTE parameter list is displayed.

System action: See the system action for the message that precedes this one.

User response: Examine the request type, return codes, and parameter list provided in the RRSFLIST output. For mappings of the parameter lists to help you determine the cause of the error, see the z/OS Security Server RACF Diagnosis Guide.

IRRR111I  Application update has completed successfully at node node-name. Output {written to data-set-name | was sent via TSO TRANSMIT | was lost | was not requested}

Explanation: The output from an automatically directed application update was received from the execution node. The output was returned in the described manner or could not be returned because of an error.

- The update to the RACF database on the target system was made successfully.
- If the output was "lost," an error occurred while attempting to return the output. For example, a workspace data set was damaged or a TRANSMIT was attempted to the JES node name.
- If the output was "not requested," the OUTPUT setting of the SET command did not specify that output should be returned.

User response: Examine the RRSFLIST data set, data-set-name, or invoke TSO RECEIVE to view the returned output. If the output was lost, contact your system programmer and report the failure. If output is available, examine the output for additional diagnostic information, such as the node affected and messages such as IRRR102I or IRRR103I. If a TRANSMIT was attempted to the JES node name, use the SET JESNODE command.

IRRR116I  Application update request was not sent for class class-name, profile name profile-name. Processing code is code.

Explanation: An error occurred during the propagation of an automatically directed application update. The update for profile profile-name in class class-name could not be sent to the intended node. This message appears in the RRSFLIST output based on the OUTPUT setting of the SET command, or is transmitted if the RRSFLIST data set is full.

System action: The RACF database is changed on the source node, but is not changed on the target node.

User response: Contact your system programmer.

System programmer response: The processing code in the error message indicates what type of error occurred. They are as follows:

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>502</td>
<td>Error obtaining storage</td>
</tr>
<tr>
<td>503</td>
<td>Error writing to a workspace data set</td>
</tr>
<tr>
<td>506</td>
<td>Update parameter list is too long</td>
</tr>
</tbody>
</table>

IRRR117I  Application update could not be sent to node node-name. Output {written to data-set-name | was sent via TSO TRANSMIT | was lost | was not requested}.

Explanation: This message is sent to a user through the TSO SEND command. It is notification of the results of an automatically directed application update. The update was intended to be sent to a target node, but an error occurred before the update could be sent. For example, the problem might have occurred while obtaining storage or performing I/O to a workspace data set.

- If the output was "lost," an error occurred while attempting to return the output. For example,
workspace data set was damaged or a TRANSMIT was attempted to the JES node name.

- If the output was "not requested," the OUTPUT setting of the SET command did not specify that output should be returned.

**User response:** If output was returned, check its contents for additional error messages, such as error message IRRR116I. There might also be additional error messages sent to the operator console or records written to the LOGREC data set. If a TRANSMIT was attempted to the JES node name, use the SET JESNODE command.

IRRR118I  Application update could not be executed at node node-name. Output [written to data-set-name I was sent via TSO TRANSMIT I was lost I was not requested].

**Explanation:** This message is sent to a user through the TSO SEND command. It is a notification of the results of an automatically directed application update. The update was sent to a target node, but an error occurred before the processing of the update on that node. For example, the target user ID might not exist or is revoked.

- If the output was "lost," an error occurred while attempting to return the output. For example, a workspace data set was damaged or a TRANSMIT was attempted to the JES node name.
- If the output was "not requested," the OUTPUT setting of the SET command did not specify that output should be returned.

**User response:** If output was returned, check its contents for additional error messages, such as error message IRRC110I, IRRC011I, or IRRC012I. There might also be additional error messages sent to the operator console or the syslog. If a TRANSMIT was attempted to the JES node name, use the SET JESNODE command.

IRRR119I  APPLICATION UPDATE type CANNOT BE SENT TO PARTNER NODE node-name (SYSNAME system-name). THIS PARTNER NODE HAS RACF LEVEL level WHICH DOES NOT SUPPORT AUTOMATIC DIRECTION OF APPLICATION UPDATES.

**Explanation:** An attempt was made to propagate an application update, or to return output from an application update to a downlevel remote node.

If type is REQUEST, the application update could not be sent to the remote partner node indicated by the RRSFDATA profiles.

If type is OUTPUT, the output produced by an application update could not be sent to the remote partner node specified by the SET command. On the last handshake with this node, the level of RACF was not high enough to accept application update requests or output. The level must at least correspond to FMID HRF2230, which is available with the OS/390 Release 3 Security Server. If SYSNAME information is present for the node name in this message, the node that precedes the SYSNAME is a multisystem node.

**System action:** If type is REQUEST, the RACF database is changed on the source node, but the request is not sent to the target node.

If type is OUTPUT, the output produced by an application update attempted on this node is not sent to the node specified by the SET command. The application update may or may not have been successfully made on this node. Additional requests and output directed to this remote partner node are discarded without any additional error messages.

If handshaking occurs again between these nodes, another error message is issued if the remote node is still at a lower level and has requests or output being directed to it.

**System programmer response:** If type is REQUEST, you should change the RRSFDATA profiles to prevent automatic direction of application updates to this remote node until it has been updated to a level of RACF that supports these requests. For additional information about RRSFDATA profiles, see z/OS Security Server RACF Security Administrator's Guide.

If type is OUTPUT, use the SET command to prevent additional output from being sent to this remote node. For additional information about the SET command, see z/OS Security Server RACF Command Language Reference.

After the remote system is updated, you must reestablish the connection with it by issuing a RESTART or TARGET command to pick up the new level.

**Destination:** Descriptor code is 6. Routing codes are 2 and 9.

**RACLINK command messages**

IRRS001I  RACF subsystem return code is return-code, reason code is reason-code.

**Explanation:** A problem occurred with the RACF subsystem while processing a RA CLINK request. This message is preceded by a message indicating what problem occurred. This message is sent to the TSO terminal of the RA CLINK issuer.

**System action:** Processing for this RA CLINK command stops.

**User response:** Refer to the documentation for the
error message that was issued before this message.

**IRRS002I**  
**RACF subsystem is not active, your request cannot be processed.**

**Explanation:** The RACF subsystem must be active for a RACLINK command to be processed. This message is sent to the TSO terminal of the RACLINK issuer.

**System action:** Processing for this RACLINK command stops.

**User response:** Contact the system operator to start the RACF subsystem.

**Operator response:** Start the RACF subsystem by issuing `START subsystem-name SUB=MSTR` from the operator's console, where `subsystem-name` is the RACF subsystem that you want to become active.

**IRRS003I**  
**Unable to communicate with the RACF subsystem. IEFSSREQ return code is return code.**

**Explanation:** The RACLINK command attempted to send a request to the RACF subsystem, but the request failed. No profiles have been updated. This message is sent to the TSO terminal of the RACLINK issuer.

**System action:** RACLINK command processing ends.

**User response:** Report this message to your system programmer.

**System programmer response:** The return code indicated in this message reflects the return code from the MVS IEFSSREQ subsystem interface. The return code may be one of these values:

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>The subsystem does not support this function.</td>
</tr>
<tr>
<td>8</td>
<td>The subsystem exists, but is not active.</td>
</tr>
<tr>
<td>12</td>
<td>The subsystem is not defined in the IEFSSNxx parmlib member.</td>
</tr>
<tr>
<td>16</td>
<td>The function has not completed. This is a disastrous error.</td>
</tr>
<tr>
<td>20</td>
<td>The SSOB or SSIB have invalid lengths or formats.</td>
</tr>
<tr>
<td>24</td>
<td>The SSI has not been initialized.</td>
</tr>
</tbody>
</table>

A return code of 4, 16, 20, or 24 indicates a RACF code problem, report this message to IBM support.

A return code of 8 or 12 indicates an installation or RACF subsystem configuration problem. See [z/OS Security Server RACF System Programmer’s Guide](https://www.ibm.com) for information about configuring the RACF subsystem.

**IRRS004I**  
**You are not authorized to use the {DEFINE | PWSYNC} keyword for node node-name. The association for userid userid with node.userid was not defined.**

**Explanation:** The RACLINK command issuer is not authorized to use the indicated keyword. The command issuer either has not been permitted to the RACLINK resource's DEFINE or PWSYNC profile, or the RRSFDATA class is not currently active. This message is sent to the TSO terminal of the RACLINK issuer.

**System action:** Processing for this RACLINK command stops. No user ID association is defined.

**User response:** Contact the RACF security administrator to permit you to the RACLINK.DEFINE node-name profile or the RACLINK.PWSYNC node-name profile in the RRSFDATA class and to ensure that the RRSFDATA class is active.

**RACF Security Administrator Response:** Permit the command issuer to the RACLINK.DEFINE node-name profile or the RACLINK.PWSYNC node-name profile in the RRSFDATA class and issue a SETROPTS command to activate the RRSFDATA class.

**IRRS005I**  
**RACLINK to associate userid userid with node.userid failed. Associations to the same userid on the same node are not permitted.**

**Explanation:** A RACLINK DEFINE command was issued to define an association with the same user ID on the same node. This message is sent to the TSO terminal of the RACLINK issuer.

**System action:** Processing for this RACLINK command stops. No user ID association is defined.

**IRRS006I**  
**The local node is not defined. RACLINK command cannot be processed.**

**Explanation:** RACF is unable to locate the local node. The local node is required for one of the following reasons:

1. To validate the use of the DEFINE keyword and the PWSYNC operand
2. As the command default, because the RACLINK command did not specify a target node.

This message is sent to the TSO terminal of the RACLINK issuer.

**System action:** Processing for this RACLINK command stops. No user ID association is defined.

**User response:** Contact your RACF security administrator to have the local node defined to the RACF remote sharing facility.
RACF Security Administrator Response: Call the system operator to issue the TARGET command to identify the local node.

IRRS007I  The RACLINK command must be authorized.

Explanation: An attempt was made to issue the RACLINK command, but RACLINK is not recognized as an authorized command. This message is sent to the TSO terminal of the RACLINK issuer.

System action: The RACLINK command being processed is unsuccessful; processing ends.

User response: Contact the system programmer.

System programmer response: The most likely cause of this problem is that RACLINK is not present in the list of authorized commands in the IKJTSOxx parmlib member currently in effect. Another possibility is that RACLINL is not in an APF-authorized library.

IRRS008I  YOU ARE NOT ALLOWED TO ISSUE THE RACLINK COMMAND AS AN OPERATOR COMMAND.

Explanation: You issued a RACLINK command as an operator command, but did not have authority for one of the following reasons:

- There is no RACF-defined user ID associated with the operator.
- A profile in the OPERCMDS class is preventing the RACLINL command from being issued by the user ID.

System action: Processing for this RACLINK command stops.

User response: If the RACLINK command was issued from an operator console, make sure that the console is logged on. If the RACLINK command was issued through some other means, make sure that the

RACLINK command or RRSF output handling task messages

IRRT003I  The (node.userid1) association could not be located in the userid2 user profile.

Explanation: A command was issued to retrieve user ID association information for node.userid1, but no user ID association for node.userid1 was located in the profile for userid2. This message is sent to the command issuer or the RRSFLIST data set of the user. If the data set is full, this message is transmitted to the TSO terminal of the user.

System action: The command being processed is unsuccessful; processing ends.

User response: Verify that the correct node and user ID were entered on the command. If they are incorrect, issue the command again with the correct node and user ID. If the node and user ID are correct and you receive this message, the user ID association must be defined before the command is successful.

IRRT004I  The requested association could not be [located | defined | deleted] because user userid is not RACF defined.

Explanation: A command was issued to retrieve user ID association information for userid, but the userid profile does not exist in the RACF database. This message is sent to the command issuer or the RRSFLIST data set of the user. If the data set is full, this message is transmitted to the TSO terminal of the user.

System action: The command being processed is unsuccessful; processing ends.

User response: Verify that the correct userid was
specified on the command. If incorrect, issue the command again with the correct user ID. If the user ID is correct, contact the security administrator to add the user ID to the database, if needed.

| IRRT005I | RACF ICHEINTY return code return-code received while attempting to [retrieve | define | delete | approve] association (node.userid) for user userid. |

**Explanation:** A command was issued to update or retrieve user ID association information for node.userid and an ICHEINTY failure occurred. This message is sent to the command issuer or the RRSFLIST data set of the user. If the data set is full, this message is transmitted to the TSO terminal of the user.

**System action:** The command being processed is unsuccessful; processing ends.

**User response:** Verify that the correct command was entered. If incorrect, issue the command again with the correct user ID association information. If the correct command was entered, contact the system programmer.

**System programmer response:** See `z/OS Security Server RACF Macros and Interfaces` to analyze the ICHEINTY return code.

| IRRT006I | Association key length length is not valid. Information cannot be retrieved for user userid. |

**Explanation:** In the command to retrieve user ID association information for user userid, the specified target node or target user ID exceeded the maximum length of 8 characters. This message is sent to the command issuer or the RRSFLIST data set of the user. If the data set is full, this message is transmitted to the TSO terminal of the user.

**System action:** The command being processed is unsuccessful; processing ends.

**User response:** Reissue the command with the correct target node and user ID.

| IRRT007I | No associations could be located in the userid user ID profile. |

**Explanation:** There are no target user ID entries in the indicated user ID profile. This message is sent to the TSO terminal of the RAELINK issuer.

**System action:** The RAELINK command processing ends and no retrieval is performed.

**User response:** Create the required associations with the RAELINK DEFINE command.

| IRRT008I | Unable to find association(s) which matched (node.userid1) for user ID userid2. |

**Explanation:** No target user ID entries match the selection criteria in userid2's profile. This message is sent to the TSO terminal of the RAELINK issuer.

**System action:** The RAELINK command processing ends and no retrieval is performed.

**User response:** Create the required associations with the RAELINK DEFINE command.

| IRRT009I | RACLINK could not be completed because target node node-name is undefined. |

**Explanation:** RACF is unable to locate the node name specified. This message is sent to the TSO terminal of the RAELINK issuer.

**System action:** The RAELINK command stops processing.

**User response:** Issue a RAELINK LIST command to determine if the association is defined or updated. Also, ensure that you spelled the node name correctly. If the node name and its associations are correct, contact your system programmer to have the remote node defined to RACF.

| IRRT010I | The definition for association (node-name.userid) in user userid profile already exists. |

**Explanation:** The user ID association that you are trying to define exists in the RACF database. This message is sent to the TSO terminal of the RAELINK issuer.

**System action:** Processing for this RAELINK command stops.

**User response:** Verify that the correct RAELINK command was entered.

| IRRT011I | [command-name | Password synchronization] was not performed by userid at node node-name. |

**Explanation:** RACF processing has determined that the indicated function could not be performed at target node node-name for target user userid. This message is accompanied by messages IRRT003I, IRRT004I, IRRT005I, IRRT006I, IRRT012I, or IRRT013I, which provide a more detailed analysis of the error. Refer to these messages for further details. This message is appended to the RRSFLIST data set of the user. If the data set is full, this message is transmitted to the TSO terminal of the user.
**System action:** The command being processed is unsuccessful; processing ends.

**User response:** Verify that the correct command was entered. If it is correct, see the accompanying messages for more information.

**IRRT012I** Association (node.userid) has not been approved.

**Explanation:** RACF processing has determined that a directed command could not be performed because the user ID association between the command issuer and target user *userid* on target node *node* has not been approved. This error occurs only when user ID association approval processing could not complete as the result of a communication failure between the participating systems. This message is appended to the RRSFLIST data set of the user. If the data set is full, this message is transmitted to the TSO terminal of the user.

**System action:** The command being processed is unsuccessful; processing ends.

**User response:** Reestablish a user ID association between the user IDs by deleting and then redefining the association. If the user ID association cannot be reestablished, contact the system programmer. The source of the communication failure must be determined. If the association was reestablished successfully, try the command again.

**System programmer response:** Communication from the target node to the source node for a directed command has been disrupted. Determine the status of the communication links from the target to the source node by issuing the TARGET LIST command on the target node. If either node is not in the OPERATIVE ACTIVE state, try to put the affected node into the operative state by issuing the TARGET command. The specific command operands depends on the state of the node. See [z/OS Security Server RACF Command Language Reference](#) for details of the TARGET command.

If communication cannot be reestablished, there is most likely a problem with the physical linkage between the systems.

**IRRT013I** The ONLYAT keyword was specified but user ID *userid* at node *node-name* does not have the SPECIAL attribute.

**Explanation:** RACF processing has determined that a directed command could not be performed because the ONLYAT keyword was specified and target user *userid* at node *node-name* does not have the SPECIAL attribute. If the ONLYAT keyword is specified, the command can be directed only to a user who has the SPECIAL attribute. This message is appended to the RRSFLIST data set of the user. If the data set is full, this message is transmitted to the TSO terminal of the user.

**System action:** The command being processed is unsuccessful; processing ends.

**User response:** Only communication between two user IDs with the SPECIAL attribute is permitted with the ONLYAT keyword. Contact the security administrator on the indicated node *node-name* to determine whether *userid* should be given the SPECIAL attribute.

**IRRT014I** RACLINK command was unable to obtain storage for the association entry.

**Explanation:** A failure occurred while attempting to obtain storage necessary to update an association entry in the local profile of the user. This message is sent to the RACLINK issuer.

**System action:** RACLINK command processing ends. The local user profile or the remote user profile has been updated.

**User response:** Notify the system programmer.

**System programmer response:** Note the message ID and any other diagnostic information generated, and contact your IBM support center.

**Problem Determination:** The storage request was for subpool 1.

**IRRT015I** (Peer | Managed) association with *userid* at node *node-name* has been approved.

**Explanation:** The indicated association with the target user ID was approved. Remote sharing requests to the target user ID can now be processed. This message is sent to the TSO terminal of the RACLINK issuer.

**System action:** The RACLINK command completes processing.

**User response:** None.

**IRRT016I** The ONLYAT keyword was specified but user ID *userid* at node *node-name* is not RACF defined.

**Explanation:** RACF ONLYAT keyword processing has determined that a command cannot be directed to *userid* at node *node-name* because *userid* is not defined to RACF. This message is appended to the RRSFLIST data set of the user. If the data set is full, this message is transmitted to the TSO terminal of the user.

**System action:** The command being processed is unsuccessful; processing ends.

**User response:** Verify that the correct user ID was specified on the command. If incorrect, issue the command again with the correct user ID. If *userid* is correct, then contact the security administrator to add the user ID to the database.
IRRT017I  userid ATTEMPTED TO ACCESS ASSOCIATION INFORMATION FOR for-user. ACCESS IS DENIED.

Explanation: The user userid entered a RACLINK command, specifying for-user for the ID keyword. User userid is not authorized to access the for-user profile.

System action: RACLINK command processing ends. No profiles are updated.

Operator response: Notify the security administrator.

RACF Security Administrator Response: If userid should have the authority to access the for-user profile, userid must have one of the following authorities:

- System SPECIAL
- SPECIAL in the group that the for-user belongs to
- OWNER of the for-user profile

Destination: Descriptor code is 4. Routing code is 9.

IRRT018I  Association node.userid cannot be approved. It is not pending approval by source-userid on node source-node-name.

Explanation: The user source-userid on node source-node-name entered a RACLINK APPROVE command, specifying node.userid as the target of the command. This association is not waiting approval by user ID source-userid on node source-node-name. The association is either already established or is waiting approval from node.userid. This message is sent to the TSO terminal of the RACLINK issuer.

System action: RACLINK command processing ends. No profiles are updated.

User response: Use the RACLINK LIST command to list the association. From the output, determine if the association is already approved or waiting approval from the target. If it is already approved, no action is required. If it is awaiting approval from the target, contact the target user and request approval for the association.

IRRT021I  Association (node-name.userid) deleted from userid user ID profile.

Explanation: The RACLINK association for the specified node and user ID has been deleted from the RACF database. This message is sent to the TSO terminal of the RACLINK issuer.

System action: The RACLINK association entry is deleted from the RACF database.

IRRT024I  Your userid userid does not have sufficient authority to access the association information of user id.

Explanation: The RACLINK command failed because the user did not have system SPECIAL, group SPECIAL for the group that owns the user ID specified on the ID keyword, and is not the owner of the user ID specified on the ID keyword. This message is sent to the RACLINK issuer.

System action: RACLINK command processing ends.

User response: If you need authority to issue the RACLINK command with the ID keyword or to access the association information for user userid, contact your RACF security administrator.

IRRT026I  RACLINK command failure. Unexpected request request was received. Reason code is reason-code.

Explanation: An internal error occurred while processing a RACLINK request. This message is sent to the RACLINK issuer.

System action: RACLINK command stops processing.

User response: Contact the IBM support center to report the problem.

Code Explanation
1 Define processing received an unknown request.
2 General RACLINK processing received an unknown request.

IRRT030I  RACLINK PROCESSING ERROR. [INPUT IS NOT CORRECT | REQUEST TYPE IS NOT CORRECT ]

Explanation: The input to the RACLINK task handler is not correct. Typical causes are:

- Input specified on the RACLINK command was incorrect.
- The request type received was not RACLINK-related.

There may be an internal problem.

System action: Processing for this RACLINK command stops.

User response: Contact your system programmer.

System programmer response: Contact the IBM service center to report this problem.

Destination: Descriptor code is 4. Routing codes are 2 and 9.

IRRT031I  RACLINK command awaiting approval from userid at this node. Association requested by node-name.userid.

Explanation: The RACLINK association is pending approval from the specified user ID. This message is sent to the RACLINK issuer.

System action: The RACLINK command is on hold until approval.

User response: Wait until the RACLINK association is
approved or contact the owner of the user ID to issue the approval.

**Problem Determination:** For information about the pending association waiting for your approval, use the `RACLINK LIST` function.

**IRRT032I** RACLINK command to associate user ID *userid* with *node-name*. *userid* is pending approval.

**Explanation:** The RACLINK association is pending approval from the specified user ID. The association could be pending for one of the following reasons:

- The association is waiting approval from the target.
- The conversation between the local and target nodes is not active.
- The RACLINK command is pending for some other reason. A message will follow.

This message is sent to the RACLINK issuer.

**System action:** The RACLINK command continues processing. If the target node is not active, the RACLINK request is held in the OUTMSG file until the node is made OPERATIVE. After the node becomes OPERATIVE, the RACLINK command continues processing.

**User response:** Other messages usually follow this one indicating the status of the RACLINK request. If no other messages follow, contact the owner of the target user ID to determine if the RACLINK request reached the target user ID. If the RACLINK request reached the target user ID, the target user ID can approve the association using the RACLINK APPROVE command. If the association did not get approved, the target user must issue a RACLINK APPROVE command.

**System programmer response:** Query the status of the communication link between the two nodes by issuing the `TARGET LIST` command. The node must be made OPERATIVE in order for the RACLINK request to be processed.

**IRRT034I** All associations of RACLINK command issuer not sent to target node *node-name*. Number associations were sent.

**Explanation:** There is a limit to the number of user IDs that may be sent to the target node at one time. That limit is indicated by *number* in the message. This message is sent to the RACLINK issuer.

**User response:** To determine what user IDs were sent to the target node, issue the `RACLINK LIST` command to display the user ID associations of the user ID. The display shows the user ID and node of each association. The first *number* user IDs on the indicated *node-name* were sent to the target node. If the association did not get approved, the target user must issue a RACLINK APPROVE command.

**IRRT042I** *subsystem-name* SUBSYSTEM WAS UNABLE TO ISSUE IEFSSREQ REQUEST. RETURN CODE IS: *return-code*.

**Explanation:** The RACLINK command attempted to send a request to the MVS IEFSSREQ subsystem and the request failed. No profiles have been updated.

**System action:** RACLINK command processing ends.

**User response:** Report this message to your system programmer.

**System programmer response:** The return code indicated in this message reflects the return code from the MVS IEFSSREQ subsystem interface. The return code may be one of these values:

<table>
<thead>
<tr>
<th>Code</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>The subsystem does not support this function.</td>
</tr>
<tr>
<td>8</td>
<td>The subsystem exists, but is not active.</td>
</tr>
<tr>
<td>12</td>
<td>The subsystem is not defined in the IEFSSNxx parmlib member.</td>
</tr>
<tr>
<td>16</td>
<td>The function has not completed. This is a disastrous error.</td>
</tr>
<tr>
<td>20</td>
<td>The SSOB or SSIB have incorrect lengths or formats.</td>
</tr>
<tr>
<td>24</td>
<td>The SSI has not been initialized.</td>
</tr>
</tbody>
</table>

A return code of 4, 16, 20 or 24 indicates a RACF code problem. Report this message to the IBM support center.

A return code of 8 or 12 indicates an installation or RACF subsystem configuration problem. See the `z/OS Migration` and `z/OS Security Server RACF System Programmer's Guide` for configuration considerations for the RACF subsystem.

**Destination:** Descriptor code is 4. Routing codes are 2 and 9.
IRRT043I  subsystem-name SUBSYSTEM IEFSSREQ REQUEST ENDED WITH A RETURN CODE OF return-code.

Explanation: An attempt to send a request to the MVS IEFSSREQ subsystem interface failed. No profiles have been updated.

System action: RACLINK command processing ends.

Operator response: Report this message to your system programmer.

System programmer response: The return code indicated in this message is the value of the SSOBRETN field in the option block (SSOB) of the subsystem. The return code may be one of these values:

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>The subsystem could not execute the command because of an internal parameter error, or the subsystem supports this request, but is not active.</td>
</tr>
<tr>
<td>16</td>
<td>The caller is not APF-authorized, or storage is unavailable for an internal data area.</td>
</tr>
</tbody>
</table>

File allocation messages

IRRU080I  subsystem-name RACF VSAM FILE OPEN AND CLOSE PROGRAM ENCOUNTERED AN ERROR. ABEND CODE IS abend-code.

Explanation: The subsystem task that holds all the VSAM OPENs for the subsystem encountered an error. This message is written to the SYSLOG.

System action: The task attempts to restore an operational state by ignoring the current request and moving to the next request.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. For a complete discussion, see z/OS Security Server RACF Diagnosis Guide.

Operator response: Report this message to your system programmer.

Problem Determination: If the abend code is ???-??, then no SDWA was provided and RACF could not determine the abend code.

For an explanation of these codes, see z/OS MVS System Codes.

IRRU081I  subsystem-name RACF VSAM FILE OPEN AND CLOSE PROGRAM ENCOUNTERED AN ERROR. ABEND CODE IS abend-code. PROGRAM ENDING.

Explanation: The subsystem task that holds all the VSAM OPENs for the subsystem had an error.

This message appears when an abnormal situation that cannot be recovered from occurs.

System action: The program releases all system resources it holds, this includes closing all VSAM files, posting all tasks waiting on this program and then ends. The subsystem attempts to restart the file program.

When an RRSF subtask ends processing, its owning task restarts the subtask and, depending on the type of abend, the subtask should resume processing any work in its input queue. For a complete discussion, see z/OS Security Server RACF Diagnosis Guide.

Operator response: Report the occurrence of the message to the system programmer.

Problem Determination: If the abend code is ???-??, then no SDWA was provided and RACF could not determine the abend code.

For an explanation of these codes, see z/OS MVS System Codes.

Destination: Descriptor code is 6. Routing code is 2.
RRSF enveloping messages

**IRRVO001I** RACF command envelope ended in abend processing.

**Explanation:** An internal error occurred. RACF experienced an abend while handling a prior abend. The initial abend code should be listed in message **IRRVO080**, which was issued before this one. This message is sent to the user's TSO terminal or the operator console, depending on where the command was issued, or this message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

**System action:** Processing is halted at the time of the abend.

**User response:** If you were performing an update type command (for example, ALTUSER), you can use the appropriate list command (for example, LISTUSER) to determine if the update occurred before the abend. If the problem persists, contact your RACF support personnel and report the abends to the IBM support center. Be sure to indicate the abend code and reason code that were reported in the message.

**Problem Determination:** Examine the console log and the system abend dump for more information pertaining to the abends.

**IRRVO002I** Node *nodename* is not defined to RACF or is not available.

**Explanation:** An attempt was made to direct a RACF command to a node that has not been defined or that is unavailable. *nodename* might appear as an asterisk (*) if you used shorthand notation to direct a command to the local node (for example, AT(userid)) and had not defined a local node. This message is sent to the user's TSO terminal.

**System action:** This message is followed by message **IRRVO05I**, which indicates that the command will not be sent to node *nodename*. If the AT (or ONLYAT) keyword specified other nodes that are defined and available, the command is still processed on those nodes.

**User response:** If you made an error while entering the node name, reissue the command with the correct node name. Otherwise, contact your RACF security administrator to determine whether the node is defined and, if so, why it is unavailable.

**Problem Determination:** If you are authorized to issue RACF operator commands, you can issue the TARGET LIST command to determine which nodes are defined to your system.

**IRRVO003I** YOU ARE NOT ALLOWED TO ISSUE THE command COMMAND AS AN OPERATOR COMMAND.

**Explanation:** You issued a RACF command as an operator command, but did not have authority for one of the following reasons:

- There is no RACF-defined user ID associated with the operator.
- A profile in the OPERCMDS class is preventing the command from being issued by the user ID.

**Note:** If the command you entered was a SETROPTS command, you may have READ access, which only allows you to issue SETROPTS LIST. You must have UPDATE access to issue the SETROPTS command with keywords other than LIST.

**System action:** Processing for this command stops.

**User response:** If the command was issued from an operator console, make sure that the console is logged on. If the command was issued through some other means, make sure that the command is issued from a RACF-defined user ID.

If you received an ICH408I message before this message, an OPERCMDS profile is preventing access. Contact your RACF security administrator to get access to the OPERCMDS profile.

**RACF Security Administrator Response:** If appropriate, permit the user ID to the OPERCMDS profile that is protecting the command in question.

**Destination:** Descriptor code is 6. Routing code is 2.

**IRRVO004I** Unexpected return code *return-code* received from node name and user ID verification.

**Explanation:** Because of an internal error, RACF was unable to properly verify the node name and user ID being processed. This message is issued from the IRRENV04 CSECT when an unknown return code is returned from the node name and user ID verification service. This message is sent to the user's TSO terminal.

**System action:** This message is followed by message **IRRVO05I**, which indicates that the command will not be sent to the specified node. If the AT (or ONLYAT) keyword specified other nodes to direct the command to, those other nodes are still processed.

**User response:** Try directing the command again to the node and user ID. If it fails, contact your RACF support personnel and report the problem to the IBM support center. Be sure to indicate the return code from this message.

**IRRVO005I** Command *RACF-command* will not be sent to node *nodename*.

**Explanation:** An error prevented RACF from directing
the command to the specified node. This message follows another message that describes in more detail why the command will not be sent. nodename might appear as an asterisk (*) if you used shorthand notation to direct a command to the local node (for example, AT(userid)) and had not defined a local node. This message is sent to the user's TSO terminal.

System action: The command is not sent to the specified node. If the AT (or ONLYAT) keyword specified that the command be directed to other nodes, those other nodes are still processed.

User response: See the message that was issued before message IRRV005I. It should describe why the command was not sent.

IRRV006I Unexpected return code return-code received from the parse of command RACF-command.

Explanation: RACF was not able to properly parse the command because of an internal logic error. This message is sent to the user's TSO terminal or the operator console, depending on where the command was issued, or this message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

It is possible that while altering the CSDATA segment, a custom field, which existed when the command was initiated, has now been deleted. In this case, issue the IRRDPI00 LIST command to check which custom fields are currently being used, and then reissue the command or contact your security administrator.

System action: The command ends processing.

User response: Contact your RACF support personnel and report the problem to the IBM support center. Be sure to indicate the return code from this message and any other associated messages.

IRRV007I Node nodename is not active.

Explanation: An attempt was made to direct a RACF command to a node that is not currently active. This message is for your information only to warn you that there may be a delay before the command actually runs at the target node. This message is sent to the user's TSO terminal.

System action: RACF sends the command request to the RACF subsystem where it will be saved. Message IRRV008I follows this message to indicate that the command will be saved. Once the target node is made operative, the saved commands will be processed. Your commands will be processed in the same order as you issued them.

User response: None required. However, if you need the RACF command change to take effect immediately, do one of the following:

- Contact the system programmer to activate the node.

- Issue the command directly on the target system. This requires you to log on to the target node and issue the command without the AT (or ONLYAT) keyword.

IRRV008I Command RACF-command will be queued for later transmission to node nodename.

Explanation: This message is for your information only to warn you that there may be a delay before the command actually runs at the target node. Message IRRV007I, which was issued before this message, should tell you why the command is being queued. This message is sent to the user's TSO terminal.

System action: RACF sends the command request to the RACF subsystem where it will be saved.

User response: None required. However, if you need the RACF command change to take effect immediately, do one of the following:

- Have your RACF personnel make the target node operative so the command runs.
- Issue the command directly on the target system. This requires you to log on to the target node and issue the command without the AT (or ONLYAT) keyword.

IRRV009I Authorization failed for the ONLYAT keyword.

Explanation: The ONLYAT keyword was specified, but you are not authorized to use it. The following requirements must be met for you to specify the ONLYAT keyword:

- You must have RACF system SPECIAL authority.
- The target user ID must have RACF system SPECIAL authority.
- If the target user ID is different from your user ID, a user ID association between your user ID and the target user ID is required.

This message is sent to the user's TSO terminal.

System action: Command processing fails to complete.

User response: Ensure all of the above requirements are met and reissue the command.

IRRV012I Association exists, but has not been approved.

Explanation: An attempt was made to direct a RACF command to a remote node. To direct such a command, you must have an approved association between the issuing user ID on the source node and the target user ID on the remote node. In this case, an association does exist between the user IDs, but the association has not been approved. This message is sent to the user's TSO terminal.
**System action:** This message is followed by message IRRV005, which indicates that the command will not be sent to the specified node. If the AT (or ONLYAT) keyword specified other nodes to direct the command to, those other nodes are still processed.

**User response:** If you made a typographical error while entering the node name or target user ID, reissue the command and enter the correct node name and target user ID. Otherwise, if the association is valid (that is, both parties agree it should be allowed), you must have the association approved. If you have the authority, use the RACLINK LIST command to determine who must approve the association. If you must approve the association, use the RACLINK command to APPROVE the association. If you do not have the authority, contact your administrator or the target user and have them use the RACLINK command to APPROVE the association.

If you need more information about the authorization requirements for using the ONLYAT keyword, see Security Server RACF Security Administrator's Guide.

**Problem Determination:** Use the RACLINK command to LIST the associations for the user ID. This can be done on each system to see what state each system thinks the relationship is in. Remember to use the ID() keyword to LIST the association if the association is for a user ID other than your own. If you try the RACLINK command with the APPROVE keyword, and the RACLINK LIST command still shows the association as PENDING APPROVAL, you should contact your RACF support personnel and report the problem to the IBM support center.

**Explanation:** An attempt was made to run a command containing the AT or the ONLYAT keyword in the RACF parameter library, from the operator console, or from the IRRSEQ00 callable service. These keywords cannot be used to direct commands that run in the RACF parameter library or are entered from the operator console or the IRRSEQ00 callable service.

**System action:** The command is ignored. Message IRRV013I is also issued to provide more information.

**User response:** If the command is in the RACF parameter library, remove the command from the RACF parameter library. If you want the command to run automatically, you must remove the AT or ONLYAT keyword and place the command in the RACF parameter library of the system you would like it to execute on.

If the command was issued from the operator console, issue the command from TSO, or issue the command without the AT or ONLYAT keyword from an operator console attached to the system where it is supposed to execute.

If the command was entered from the IRRSEQ00 callable service, issue the command from the callable service without the AT or ONLYAT keyword.

**Destination:** Descriptor code is 6. Routing code is 2.

**Explanation:** An attempt was made to run a command containing the AT or the ONLYAT keyword in the RACF parameter library, from the operator console, or from the IRRSEQ00 callable service. These keywords cannot be used to direct commands that run in the RACF parameter library or are entered from the operator console or the IRRSEQ00 callable service.

**System action:** The command is ignored. Message IRRV013I is also issued to provide more information.

**User response:** If the command is in the RACF parameter library, remove the command from the RACF parameter library. If you want the command to run automatically, you must remove the AT or ONLYAT keyword and place the command in the RACF parameter library of the system you would like it to execute on.

If the command was issued from the operator console, issue the command from TSO, or issue the command without the AT or ONLYAT keyword from an operator console attached to the system where it is supposed to execute.

**Destination:** Descriptor code is 6. Routing code is 2.

**Explanation:** You attempted to direct a RACF command to a RACF node by way of the AT() keyword, but are not authorized to do so. This message is sent to the user's TSO terminal.

**System action:** The command is not to be sent to the specified node. If the AT keyword specified other nodes to direct the command to, those other nodes are still processed.

**User response:** Contact your RACF security administrator. The users that are allowed to use the AT keyword are determined by the installation.
Problem Determination: The ability to direct commands with the AT keyword is protected by way of RACF profiles in the RRSFDATA class. Ensure that the RRSFDATA class is active, profiles are up to date (that is, RACTION REFRESHed if you have the class RACLISTed), and that you have the proper authority granted to the profile covering the "DIRECT.nodename" entity. For more details, see [z/OS Security Server RACF Security Administrator's Guide](#).

**IRR016I** Unable to communicate with the RACF subsystem. IEFSSREQ return code is `return-code`.

Explanation: An internal error occurred. RACF received an unexpected return code while attempting to communicate with the RACF subsystem. The communication is by way of the JES subsystem interface service provided by the IEFSSREQ macro. This message is sent to the user's TSO terminal.

System action: Processing is halted after the unexpected return code is received. Message IRR017I follows and informs the issuer that the command cannot be sent to the target node.

User response: In most cases, the command is not directed to the target nodes. If you were directing the command to multiple nodes, it is possible for you to get stuck in a timing situation where the first target was processed, and the second one was not. In this case, you may use the appropriate list command (for example, LISTUSER) to determine if the update occurred on any specific node. Reissue the command. If the problem persists, contact your RACF support personnel and report the return code.

Problem Determination: If you are receiving return code 4, it is likely that someone at your installation has shut down the RACF subsystem. Contact your RACF support personnel and report the return code. If you are receiving another return code, look it up in [z/OS MVS Using the Subsystem Interface](#). If you have never had the RACF subsystem successfully running, this may help you determine the problem. If you have had it running and this problem just surfaced, report it to the IBM support center. Be sure to indicate the return code that was reported in the message.

**IRR018I** Commands cannot be directed to the manager of a user ID association.

Explanation: The target user ID of a directed command is the manager of the user ID association between the command issuer and the target user ID. The managed user ID cannot direct a command to the manager of the user ID association. This message is sent to the user's TSO terminal.

System action: The command being processed is unsuccessful; processing ends.

User response: If command direction between the two user IDs is wanted, redefine the association as peer if you have sufficient authority, or contact the security administrator.
Chapter 6. IRR messages for commands, utilities, and other tasks

---

**IRRV019I**  CLIST keyword is incorrect when SEARCH command operates in RACF subsystem.

**Explanation:** AT or ONLYAT was specified along with the CLIST keyword on the SEARCH command. This is not allowed. This message is sent to the user's TSO terminal or the operator console, depending on where the command was issued.

**System action:** RACF rejects the command.

**User response:** Reissue the SEARCH command, either without the CLIST keyword or without either of the following: AT or ONLYAT.

---

**IRRV020I**  User ID association retrieval failed during command direction processing.

**Explanation:** RACF processing has determined that a command cannot be directed to the requested user and node because an error occurred while attempting to retrieve user ID association information for the command issuer. This message is accompanied by messages IRRT003I, IRRT004I, IRRT005I, or IRRT006I, which provide a more detailed analysis of the error. Refer to these messages for further details. This message is sent to the user's TSO terminal.

**System action:** The command being processed is unsuccessful; processing ends.

**User response:** Verify that the correct command was entered. If it is correct, refer to the message accompanying IRRV020I for more information.

---

**IRRV021I**  Command name changed by RACF installation exit IRREVX01. Command will not be processed.

**Explanation:** The installation command exit, IRREVX01, changed the name of the command issued in the command buffer. This is not allowed.

**System action:** Command processing stops. The command return code is set to 12 and the installation exit is called again with a post-processing call to allow processing cleanup to occur.

**User response:** Contact your system programmer to report this message.

---

**IRRV022I**  Command failed by exit. exit-text

**Explanation:** The installation command exit, IRREVX01, has requested that the command fail. The exit can provide additional information in the exit-text.

**System action:** Command processing stops. The command return code is set to 8 and the installation exit is called again with a post-processing call to allow clean up processing to occur.

**User response:** If the exit-text does not explain the cause of the failure, contact your RACF administrator or system programmer.

---

**IRRV080I**  RACF command envelope encountered an error. Abend code is abend-code-abend-reason-code.

**Explanation:** An abend was encountered while attempting to run a RACF command. The command may or may not have run before the abend was encountered. This message is sent to the user's TSO terminal or the operator console, depending on where the command was issued, or this message is appended to the user's RRSFLIST data set. If the data set is full, this message is transmitted to the user's TSO terminal.

**System action:** Processing is halted at the time of the abend.

**User response:** If you were performing an update command (for example, ALTUSER), you may use the appropriate list command (for example, LISTUSER) to determine if the update occurred before the abend. If the problem persists, contact your RACF support personnel and report the problem to the IBM support center. Be sure to indicate the abend code and reason code that were reported in the message.

**Problem Determination:** Examine the console log and the system abend dump for more information pertaining to the abend.

---

**IRRV098I**  <internal command buffer>

**Explanation:** The entire text of this message is an insert. This message is for diagnostic purposes only. It may look different each time it is issued.

The message is issued each time an internal command buffer gets rebuilt. This can be useful when diagnosing command errors. It provides a step-by-step history of how the command text is assembled. These messages are issued only when the RACF subsystem SET command is used to activate the TRACE(IMAGE) option, and a user issues a RACF command that ends in the three characters “-c”. This message is sent to the user's TSO terminal or the operator console, depending on where the command was issued.

**System action:** The command processes normally even though the command trace was requested.

**Problem Determination:** You should get these messages only when IBM has asked you to turn on the trace options described above in the “Explanation” section. Save the messages and report them to the IBM support center. Remember to turn off the trace option by using the SET command with the TRACE(NOIMAGE) keyword.

---
IRR099I  <internal command buffer>

Explanation: The entire text of this message is an insert. This message is for diagnostic purposes only. It may look different each time it is issued.

The message is issued each time an internal command buffer gets rebuilt. This can be useful when diagnosing command errors. It provides a step-by-step history of how the command text is assembled. In addition, this message is used to trace which TSO macros are being used during the parsing of the RACF command. These messages are issued only when the RACF subsystem SET command is used to activate the TRACE(IMAGE) option, and a user issues a RACF command that ends in the three characters “-t”. This message is sent to the user’s TSO terminal or the operator console, depending on where the command was issued.

System action: The command processes normally even though the command trace was requested.

Problem Determination: You should get these messages only when IBM has asked you to turn on the trace options described above in the “Explanation” section. Save the messages and report them to the IBM support center. Remember to turn off the trace option by using the SET command with the TRACE(NOIMAGE) keyword.

RACPRIV command messages

IRRW001I The functions of the RACPRIV command are not available.

Explanation: One of the following occurred:

- RACF is not active
- The write-down by user option is not active

System action: RACPRIV command processing ends.

User response: See your RACF security administrator.

Deleting RACPRIV command messages

IRRW002I You are not authorized to issue the RACPRIV command.

Explanation: You are not defined to RACF with sufficient authority and cannot issue the RACPRIV command.

System action: RACPRIV command processing ends.

User response: See your RACF security administrator.

RACMAP command messages

IRRW201I You are not authorized to issue the RACMAP command.

Explanation: One of the following conditions occurred:

- RACF is not active.
- You do not have the required authority to issue the RACMAP command.

System action: RACMAP command processing ends.

User response: Contact the RACF security administrator. See z/OS Security Server RACF Command Language Reference for more information about the authority required to issue the command.

IRRW202I The user ID specified is not defined to RACF.

Explanation: The user ID specified on the ID keyword of the RACMAP command could not be found in the RACF database.

System action: RACMAP command processing ends.

User response: Ensure that the user ID is specified correctly and that the user is defined to RACF. Issue the command again.

IRRW203I Unexpected ICHEINTY error encountered during command processing. ICHEINTY RC = x’rercode’, ICHEINTY RSN = x’rsncode’.

Explanation: During command processing, RACPRIV called the R_writepriv callable service, and received a return code and reason code that were not expected.

System action: RACPRIV command processing ends.

User response: Report this error to the system programmer and provide the exact text of the command you issued.

System programmer response: Use the return and reason code information in z/OS Security Server RACF Callable Services to determine the error condition and fix the error. If necessary, report the problem to the IBM Support Center.


**ICHEINTY RSN = x'rsncode'.**

**Explanation:** During command processing RACMAP issued an ICHEINTY and received a return code and reason code that were not expected.

**System action:** RACMAP command processing ends.

**User response:** Report this message to the system programmer and provide the exact text of the command you issued.

**System programmer response:** Use the return code information in [z/OS Security Server RACF Macros and Interfaces](https://www.ibm.com/support/docview/groups/pdf_16731) to determine the error condition and fix the error.

---

**IRRW204I** No information was found for user *userid*.

**Explanation:** RACMAP was unable to find distributed identity information for the user ID that is indicated in the message.

**System action:** RACMAP command processing ends.

**User response:** Ensure that the ID keyword is specified correctly.

---

**IRRW205I** Additional information is required to identify the identity mapping.

**Explanation:** RACMAP found more than one distributed identity mapping for this user. The information required to uniquely identify the mapping was not provided.

**System action:** RACMAP command processing ends.

**User response:** Provide the label of the mapping to be deleted. You can issue the RACMAP LISTMAP to determine the mapping label.

---

**IRRW206I** No matching identity mapping was found for this user.

**Explanation:** RACMAP could not find a mapping profile for the specified user that matched the label provided.

**System action:** RACMAP command processing ends.

**User response:** Ensure that the ID keyword and LABEL keyword are specified correctly. The value for the LABEL keyword must be specified in the same case and include any blank characters as shown by the RACMAP LISTMAP command.

---

**IRRW207I** Unexpected RACROUTE REQUEST= request-type error encountered during command processing. SAF RC = x'retcode', RACF RC = x'retcode', RACF RSN = x'rsncode'.

**Explanation:** During command processing RACMAP issued a RACROUTE request of the specified type but received an unexpected return code and reason code.

**System action:** RACMAP command processing ends.

**User response:** Report this message to the system programmer and provide the exact text of the command you issued.

**System programmer response:** Use the return code information in [z/OS Security Server RACROUTE Macro Reference](https://www.ibm.com/support/docview/groups/pdf_16731) to determine the error condition and fix the error.

---

**IRRW208I** The label *label-name* is already in use.

**Explanation:** You attempted to associate a user ID with a mapping profile and assign *label-name* to that association. This label is already in use for this user ID.

**System action:** RACMAP command processing ends.

**User response:** Specify a different label and reissue the command.

---

**IRRW209I** This filter already exists. It cannot be added.

**Explanation:** You attempted to add a filter that already exists in a mapping profile in the IDIDMAP class. Filters must be unique.

**System action:** RACMAP command processing ends.

**User response:** Specify a different filter value, or delete the existing mapping profile, and reissue the command.

---

**IRRW210I** RACLISTed profiles for the IDIDMAP class will not reflect changes until a SETROPTS RACLIST REFRESH is issued.

**Explanation:** RACF uses copies of the IDIDMAP profiles that exist in a dataspace. Updates made to IDIDMAP profiles become effective only when the SETROPTS command is issued with the REFRESH operand. Until then, any updates are not used by RACF.

**System action:** RACMAP command processing continues.

**User response:** Issue the following command to update the dataspace copies of the profiles:

```
SETR RACLIST(IDIDMAP)REFRESH
```

If issuing this RACMAP command does not change anything, it is not necessary to use the SETROPTS REFRESH command to update profiles that have been processed with the RACLIST command.
IRRW211I Registry information is required.

Explanation: You specified a MAP request, but did not specify the registry name.

System action: RACMAP command processing ends.

User response: Reissue the command with the REGISTRY keyword specifying the registry name.

IRRW212I Distributed user identity information is required.

Explanation: You specified a MAP request, but did not specify the distributed user identity information.

System action: RACMAP command processing ends.

User response: Reissue the command with the USERDIDFILTER keyword specifying the distributed user identity information.

IRRW213I An error occurred while converting the data for the keyword-name keyword from EBCDIC to UTF-8.

Explanation: While converting the value specified for the USERDIDFILTER or REGISTRY keyword, from EBCDIC format to UTF-8 format, the UNICODE services returned an unexpected return code. The value specified might contain multibyte characters causing the value to exceed the byte limit. After conversion, the USERDIDFILTER value cannot exceed 246 bytes and the REGISTRY value cannot exceed 255 bytes.

System action: RACMAP command processing ends.

User response: Check the characters in the specified keyword to see if they require more than one byte when converted to UTF-8 format.

If the characters in the specified keyword require more than one byte, you can remove the qualifiers from the USERDIDFILTER keyword. You can also reduce the number of bytes used by changing the naming conventions used for X.500 distinguished names or registry names.

IRRW214I The Keyword-Name keyword is ignored when specified with the Function-Name function.

Explanation: You specified a keyword that is not needed by the function.

System action: Command processing continues.

User response: Do not do anything now, however, the next time you issue the command you can avoid specifying this keyword.

IRRW215I No user ID found associated with the specified USERDIDFILTER and REGISTRY name.

Explanation: The information you provided with the USERDIDFILTER and REGISTRY names is not associated with any RACF user ID.

System action: Command processing ends.

User response: If you want to define a distributed identity filter that is associated with this USERDIDFILTER and REGISTRY name, use the RACMAP MAP function.

IRRW216I Unexpected Callable-Service-Name callable service error encountered during command processing. SAF RC = x'\text{RetCode}', RACF RC = x'\text{RetCode}', RACF RSN = x'\text{RsnCode}'.

Explanation: During command processing, RACMAP issued a call to this callable service and received a return code and reason code that were not expected.

System action: Command processing ends.

User response: Report this message to the system programmer, and provide the exact text of the command you issued.

System programmer response: Use the return code information in z/OS Security Server RACF Callable Services to determine the error condition and fix the error. If necessary, report the problem to the IBM support center.
## RRSF operational modes and coupling facility messages

### IRRX000I

**Explanation:** The indicated member is in data sharing mode. RACF uses the coupling facility and operates in an optimized mode when performing I/O.

**System action:** RACF operates in data sharing mode.

**Operator response:** None

**System programmer response:** None.

**Destination:** Descriptor code is 4. Routing code is 2.

### IRRX001I

**Explanation:** Member member-name was unsuccessful in issuing the IXLREBLD service for the coupling facility structure with return code return-code and reason code reason-code. Processing may still be successful if another member of the sysplex data sharing group is successful in issuing the IXLEERSP START service.

**System action:** A rebuild may still occur for this structure, but not on this system. This system disconnects and enters Read-Only mode.

**Operator response:** Save the system console log and notify your system programmer. See the system console for additional messages.

**System programmer response:** See the MVS documentation for further information about IXLEERSP return and reason codes and problem determination.

**Destination:** Descriptor code is 4. Routing code is 2.

### IRRX002I

**Explanation:** Member member-name was unsuccessful in issuing the IXLEERSP service for the coupling facility structure with return code retcode and reason code rsncode.

**System action:** The RACF member member-name enters or remains in read-only mode. If you receive the message REBUILD IS IN PROGRESS, the connection was conditionally successful but this system disconnects because the structure is being rebuilt by other systems of the sysplex. This allows the rebuild to finish first.

**Operator response:** Save the system console log and notify your system programmer. See the system console for additional messages.

**System programmer response:** See z/OS MVS Programming: Sysplex Services Reference for further information about IXLEERSP return and reason codes and problem determination.

**Destination:** Descriptor code is 4. Routing code is 2.

### IRRX004A

**Explanation:** The RACF member member-name experienced a problem that prevented it from participating in data sharing. The member has automatically entered read-only mode to prevent destroying cache and data coherency of the data sharing group.

**System action:** The RACF member member-name enters read-only mode. If you receive the message REBUILD IS IN PROGRESS, the connection was conditionally successful but this system disconnects because the structure is being rebuilt by other systems of the sysplex. This allows the rebuild to finish first.

**Operator response:** Save the system console log and notify your system programmer. See the system console for additional messages.

**System programmer response:** See z/OS Security Server RACF System Programmer's Guide for further information about IXLCONN return and reason codes and problem determination.

**Destination:** Descriptor code is 4. Routing code is 2.
System action: RACF enters read-only mode. Updates to the RACF databases are not allowed from this system.

Operator response: Notify your system programmer.

System programmer response: See the system console for additional error messages and determine the cause of the problem and correct it. For details on CF recovery, see [z/OS Security Server RACF System Programmer’s Guide](#).

Destination: Descriptor code is 2. Routing code is 2.

---

IRRX005I MEMBER memname IS IN NON-DATA SHARING MODE.

Explanation: The indicated member is in non-data sharing mode. RACF does not use the coupling facility. It uses RESERVE/RELEASE serialization. However, RACF is installed for data sharing and propagates RVARY and SETROPTS commands.

System action: RACF operates in non-data sharing mode.

Destination: Descriptor code is 4. Routing code is 2.

---

IRRX006I MEMBER memname EXPERIENCED AN ERROR WHILE PROCESSING THE command COMMAND.

Explanation: An error occurred during processing of command command for member memname. The result of the command on the member memname may be unpredictable.

System action: RACF continues operation.

Operator response: Save the system console log and notify your system programmer.

System programmer response: Examine the console log for the exact nature of the problem and take appropriate action.

Destination: Descriptor code is 4. Routing code is 2.

---

IRRX008I Rebuild for structure strname has been completed.

Explanation: The XES rebuild for structure strname has completed across the sysplex.

System action: This message is presented at the completion of the rebuild regardless of the success of the rebuild on the various members in the sysplex. Those members that process the rebuild successfully enter or remain in data sharing mode. If any other error messages are issued in association with this rebuild, those members enter or remain in read-only mode.

Operator response: If the XES rebuild was not initiated from the console, save the system console log and notify your system programmer. See the system console for additional messages.

System programmer response: See the RACF documentation on the related error messages.

Destination: Descriptor code is 4. Routing code is 2.

---

IRRX009I MEMBER memname FAILED [OPEN | READ] FOR RACF DATABASE dbname.

Explanation: I/O problems to the RACF database dbname have prevented the member memname from operating in data sharing mode.

System action: The system enters or remains in read-only mode.

Operator response: Notify your system programmer.

System programmer response: To recover from this problem, consider switching to a backup RACF database (using the RVARY SWITCH command). For complete information about recovering from this problem, see [z/OS Security Server RACF System Programmer’s Guide](#). Pay particular attention to the information about failures during I/O operations on the RACF database.

Destination: Descriptor code is 4. Routing code is 2.

---

IRRX010I MEMBER memname COULD NOT ALLOCATE SUFFICIENT STORAGE FOR THE VECTOR TOKEN DURING IXLCONN [REBUILD] OF STRUCTURE strname.

Explanation: A severe storage problem, not related to the coupling facility, exists on the system itself. Although the member is connected to the structure, it cannot use the structure, because sufficient storage for the vector token could not be obtained.

System action: The system enters or remains in read-only mode.

Operator response: Notify your system programmer.

System programmer response: If the lack of storage cannot be explained or alleviated, contact your z/OS support center. After the storage problem is corrected, either re-IPL the one system or rebuild the structure.

Destination: Descriptor code is 4. Routing code is 2.

---

IRRX011A STORAGE DEFINED IN POLICY FOR STRUCTURE strname IS LESS THAN THE MINIMUM SIZE REQUIRED BY MEMBER memname FOR DATABASE dbname.

Explanation: The RACF member memname is connected to the structure strname, but determined that the structure size allocated is less than the minimum storage size required for the database dbname.

System action: The RACF member memname enters or
remains in read-only mode. RACF remains connected to the structure strname in order to allow operator initiated rebuild requests once the policy has been updated.

**Operator response:** Notify the system programmer.

**System programmer response:** Correct the policy with sufficient storage for structure strname. See z/OS Security Server RACF System Programmer’s Guide for recommended cache structure sizes and the MVS documentation on managing the coupling facility resource policy. When this is completed, issue a rebuild for the structures to be affected by the policy change.

**Destination:** Descriptor code is 4. Routing code is 2.

---

**IRR012I** STORAGE ALLOCATED FOR STRUCTURE strname IS LESS THAN THE SPECIFIED POLICY SIZE DUE TO COUPLING FACILITY STORAGE CONSTRAINTS.

**Explanation:** RACF is connected to the indicated structure, but the structure size allocated was less than the size specified by the installation’s policy.

**Note:** This message is always issued if INITSIZE was specified in the STRUCTURE statement.

**System action:** RACF remains connected. At least the minimum size required.

- If this message is followed by IRR013A, the size does not meet the minimum size required. The system enters read-only mode.
- If no other message follows, the size meets the minimum requirements. The system enters data sharing mode.

**Operator response:** Notify the system programmer.

**System programmer response:** Reassess and update the coupling facility policy based on available resources. See z/OS Security Server RACF System Programmer’s Guide for recommended cache structure sizes and MVS documentation on managing the coupling facility resource policy. When this is completed, issue a rebuild for the structures to be affected by the policy change.

**Destination:** Descriptor code is 4. Routing code is 2.

---

**IRR015A** A LINK FAILURE WAS DETECTED BY MEMBER memname FOR STRUCTURE strname CORRESPONDING TO RACF DATABASE dbname.

**Explanation:** The RACF member memname detected a link failure to structure strname. The link failure makes this structure inaccessible by this particular member. The database associated with this structure is indicated by dbname.

**System action:** The member disconnects from the structure and enters or remains in read-only mode.

**Operator response:** See the MVS system console for related messages to this link failure. Determine the cause of the link failure and correct the problem. If necessary, contact the IBM support center.

**Destination:** Descriptor code is 4. Routing code is 2.

---

**IRR016I** RACF MEMBER memname DETECTED A COUPLING FACILITY ERROR DURING function DATABASE NAME = dbname XES STRUCTURE NAME = strname XES TOKEN = X'aaaa' XES LOCAL CACHE INDEX = X'cccc' RACF RBA = xxxxxxxx XES ERROR CODE = reason

**Explanation:** A coupling facility error was encountered during the processing of either the IXLCACHE or the IXLVECTR service on the indicated member. The function specified will be either IXLVECTR or one of the following IXLCACHE operations: READ, READ OLDNAME, WRITE, WRITE OLDNAME, WRITE ICB, CROSS INVALIDATE, DELETE, DELETE ALL, READ STATS, WRITE WHENREG, or READ NO BUFFER. If there is an IXLVECTR service failure, the indicated XES Token represents the vector token and the indicated XES Error Code represents the IXLVECTR TESTLOCALCACHE return code. If there is an IXLCACHE service failure,
the indicated XES Token represents the connection
token and the indicated XES Error Code represents the
IXLCACHE reason code. This information can be used
for error analysis by IBM support personnel.
This message will be issued for the first occurrence of
an IXLCACHE or IXLVECTR error on the indicated
structure. Subsequent errors for the same service on the
same structure will not result in this message being
issued. Occurrences of the message for that structure
will be suppressed until RACF is able to issue a
successful invocation of the service. If an error recurs
after the service has been successfully invoked, the
message will be issued again.
System action: RACF processing continues.
Operator response: Notify the system programmer.

System programmer response: Check for other
associated messages. See the MVS documentation for
the XES IXLVECTR TESTLOCALCACHE return codes
or the IXLCACHE reason codes, which were mentioned
in the message.
Destination: Descriptor code is 4. Routing code is 2.

IRRX017I  NO RESPONSE RECEIVED FROM
MEMBER memname WHILE
PROCESSING function.
Explanation: During processing of the indicated
function, a response was not received from the member
memname.
System action: RACF will continue to wait for a
response from the indicated member. Once a response
has been received, RACF deletes this message.
Operator response: This message might be received if
a member is running slower than the coordinator. If
this occurs infrequently and this message is deleted, no
action is required. If this message occurs frequently, but
is always deleted eventually, contact the IBM support
center. If this message is not deleted after a reasonable
period of time, notify the system programmer.
System programmer response: Examine the console
for the exact nature of the problem on member
memname and correct it. If the problem cannot be
corrected, member memname must be removed from the
sysplex. An IPL will be required.
Destination: Descriptor code is 2. Routing code is 1.

IRRX018I  A COMMUNICATION FAILURE
OCURRED DURING RVARY
COMMAND PROPAGATION.
MEMBER memname CAN NO LONGER
USE THE RACF DATABASE.
Explanation: An XCF communication failure occurred
during propagation of an RVARY command. Member
memname has quiesced activity against the RACF
database to process the propagated RVARY command,
but is unable to complete processing because of the
communication failure. Member memname can no
longer use the RACF database.
System action: RACF continues operation, but
member memname can no longer use the RACF
database.
Operator response: Save the system console log and
notify your system programmer.
System programmer response: Examine the console
log for the exact nature of the XCF failure. Correct the
problem and reissue the RVARY command. After
member memname processes the command, it will be
able to use the RACF database again.
Destination: Descriptor code is 4. Routing code is 2.

IRRX020I  REBUILD FOR STRUCTURE strname
ON MEMBER memname HAS BEEN
INITIATED.
Explanation: A rebuild was initiated for a RACF cache
structure. This can be caused by one of the following:
• A SETXCF operator command
• A structure failure
• The use of IXLREBLD START by an authorized
program
• A loss of connectivity where the coupling facility
resource management policy’s REBUILDPERCENT
systemweight value for that structure has been
reached.
System action: RACF participates in the rebuild
process. RACF protection remains in effect but the
database is unavailable. Processing is suspended for the
duration of the rebuild. Message IRRX008I is issued for
the same structure name when the rebuild completes.
Operator response: If the rebuild was not initiated
manually by way of the SETXCF operator command,
save the system console log and notify your system
programmer. Refer to the system console for additional
messages.
| Do not issue SETXCF to force the rebuild of a structure
| into a coupling facility that is not available to the
| system because the result is read-only mode. If SETXCF
| was issued, you must exit out of read-only mode by
| issuing RVARY DATASHARE. Therefore, RACF returns
to the original coupling facility.
Destination: Descriptor code is 4. Routing code is 2.

IRRX021I  REBUILD FOR STRUCTURE strname
ON MEMBER memname HAS BEEN
STOPPED.
Explanation: During the XES rebuild, RACF received
a rebuild stop signal. This can be caused by one of the
following:
• A SETXCF operator command
• The use of IXLREBLD STOP by an authorized program

**System action:** RACF disconnects the system from this structure and enters read-only mode.

**Operator response:** Save the system console log and notify your system programmer if the stop was not initiated from the console. See the system console for additional messages.

If the system remains in read-only mode, you can use the RVARY DATASHARE command to get RACF to attempt the connections it must return to data sharing mode.

**Destination:** Descriptor code is 4. Routing code is 2.
Chapter 7. IRR messages for callable services

R_PKIServ callable service messages

IRR201I Subject name missing from certificate request.

Explanation: Either you attempted to request a PKI Services digital certificate using the R_PKIServ callable service GENCERT or REQCERT functions or you attempted to modify an existing certificate request using the R_PKIServ callable service MODIFYREQS function but did not provide a subject's name.

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: Check that you have provided some name information for the request, for example common name or title, or contact your system programmer or web page administrator.

Application Programmer Response: Check that the application invoking the R_PKIServ callable service is providing name information. (At least one of CommonName, Title, OrgUnit, Org, Locality, StateProv, or Country.)

Web Page Administrator Response: If R_PKIServ is being invoked from the PKI Services CGIs, make sure the certificate template definition in the pkiserv.tmpl file either permits the user to enter name information or the name information is present in the <CONSTANT> section.

IRR202I Hostid mapping information is too large.

Explanation: Either you attempted to request a PKI Services digital certificate using the R_PKIServ callable service GENCERT or REQCERT functions or you attempted to modify a PKI Services certificate request using the R_PKIServ callable service MODIFYREQS function but provided more than 1024 characters worth of Hostid mapping information. The total that is compared against the 1024 character limit is calculated by the following formula:

Total=Sum of (length of each subject-id@host-name specification +1) -1

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User and Administrator Response: Check that the values you have provided for the Hostid mapping fields do not total more than 1024 characters.

IRR203I Subject's name exceeds the maximum allowed (1024 characters).

Explanation: A user is attempting to perform one of the following tasks:

1. Request a PKI Services digital certificate using the R_PKIServ callable service GENCERT or REQCERT functions.
2. Preregister a client for a PKI Services digital certificate using the R_PKIServ callable service PREREGISTER.
3. Modify an existing certificate request using the R_PKIServ callable service MODIFYREQS function.

However, the subject's name value provided is too long.

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: Reduce the length of the name information for the request such as common name, title, and so on, or contact your system programmer or web page administrator.

Application Programmer Response: Modify the application invoking the R_PKIServ callable service to provide less name information.

Web Page Administrator Response: If R_PKIServ is being invoked from the PKI Services CGIs, modify the certificate template definition in the pkiserv.tmpl file to provide less name information in the <CONSTANT> section.

IRR204I "PublicKey" encoding is not valid.

Explanation: You attempted to request a PKI Services digital certificate using the R_PKIServ callable service GENCERT or REQCERT functions. The certificate request containing the public key to be certified contains an unsupported character in the Subject Distinguished Name or it does not have a valid format. It must be a base64 encoded PKCS #10 certificate request or one generated internally by your web browser.

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: If you are requesting a server certificate, make sure that the request was generated in the correct format and it does not contain unsupported characters. If you are requesting a browser certificate, make sure that you are using a supported web browser. For more information, see z/OS Cryptographic Services PKI Services Guide and Reference.
IRRD205I "PublicKey" encoding does not have a valid signature.

Explanation: You attempted to request a PKI Services digital certificate using the R_PKIServ callable service GENCERT or REQCERT functions. The certificate request containing the public key to be certified does not have a valid signature. The certificate request might have been altered.

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: If the certificate has been altered, obtain an unaltered copy and try the request again.

IRRD206I "PublicKey" encoding contains an unsupported encryption algorithm.

Explanation: You attempted to request a PKI Services digital certificate using the R_PKIServ callable service GENCERT or REQCERT functions. The certificate request containing the public key to be certified was signed using an unsupported encryption algorithm.

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: If you are requesting a server certificate, make sure that the request was generated using a supported algorithm. If you are requesting a browser certificate, make sure that you are using a supported web browser. For more information, see z/OS Cryptographic Services PKI Services Guide and Reference.

IRRD207I Incorrect KeyUsage specified.

Explanation: Either you attempted to request a PKI Services digital certificate using the R_PKIServ callable service GENCERT or REQCERT functions or you attempted to modify an existing certificate request using the R_PKIServ callable service MODIFYREQS function but provided an incorrect combination of KeyUsage values.

For RSA key types, if you specify the KeyUsage through keywords or PKI Services web page dialogs, the KeyUsages CERTSIGN, KEYCERTSIGN, or CRLSIGN cannot be specified in combination with either HANDSHAKE, KEYENCIPHERMENT, KEYENCIPHER, KEYENCRYPT, DATAENCIPHERMENT, DATAENCIPHER, or DATAENCRYPT. If you specify the KeyUsage through KeyUsage flags in a PKCS #10 certificate request, KEYCERTSIGN or CRLSIGN cannot be specified in combination with KEYAGREEMENT.

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: Select a different KeyUsage, generate a new PKCS #10 certificate, if applicable, or contact your system programmer or web page administrator.

Application Programmer Response: Modify the application invoking the R_PKIServ callable service to provide different KeyUsage values.

Web Page Administrator Response: If R_PKIServ is being invoked from the PKI Services CGIs, modify the certificate template definition in the pkiserv.tmpl file to provide different KeyUsage values in the <CONSTANT> section in the PKI templates.

IRRD208I AuthorityInfoAccess extension information is too large.

Explanation: Either you attempted to request a PKI Services digital certificate using the R_PKIServ callable service GENCERT or REQCERT functions or you attempted to modify a PKI Services certificate request using the R_PKIServ callable service MODIFYREQS function but provided more than 1024 characters worth of AuthorityInfoAccess (AuthInfoAcc) extension information. The total that is compared against the 1024 character limit is calculated by the following formula:

\[ \text{Total} = \text{Sum of (length of each AuthInfoAcc specification + 1)} - 1 \]

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: Contact your system programmer or web page administrator.

Application Programmer Response: Modify the application invoking the R_PKIServ callable service to provide less AuthInfoAcc information.

Web Page Administrator Response: If R_PKIServ is being invoked from the PKI Services CGIs, modify the <CONSTANT> section of the certificate template definition in the pkiserv.tmpl file to provide less AuthInfoAcc information.

IRRD209I Autorenew specified without NotifyEmail

Explanation: You attempted to use the MODIFYREQS function of the R_PKIServ callable service to modify a PKI Services certificate request to have automatic renewal capability. However, the request has no NotifyEmail setup.

System action: R_PKIServ processing ends.

User response: None
IRRD210I  Key generation incompatible with critical custom extension.

Explanation: You specified a custom extension with the critical flag set to C (critical) while attempting one of the following actions that involve key generation by PKI Services:

- to request a digital certificate using the GENCERT or REQCERT functions of the R_PKIServ callable service
- to modify an existing certificate request using the MODIFYREQS function of the R_PKIServ callable service

System action: R_PKIServ processing ends. RACF prevents the request from completing.

User response: Respecify the custom extension with the critical flag set to N (noncritical).

---

R_Auditx callable service messages

IRRY000I A SECURITY RELATED EVENT HAS BEEN LOGGED.

COMPONENT(component_name)
EVENT(AUTHENTICATION | AUTHORIZATION | UNSPECIFIED)
TYPE(FAILURE | WARNING)
MESSAGE(message_ID) USER(user_ID)
GROUP(group_name) [NAME(user_name)]
[CLASS(class_name)]
[PROFILE(profile_name)]

Explanation: The R_auditx callable service has logged an event to SMF on behalf of calling component component_name. The service also issued message message_ID for that component. User_ID, group_name, and user_name describe the user associated with the event. Class_name and profile_name indicate the class and profile checked to make the logging decision.

Operator response: See the related component message identified by message_ID for additional information.

System action: The event is logged to SMF.

Destination: Descriptor code is 6. Routing code is 9 and 11.
Chapter 8. IBM health checker for z/OS and sysplex messages

Health checker messages are messages issued by RACF as it manages the RACF Health Checks, such as when the RACF Health Checks are registered with the Health Check infrastructure, and which are issued by the RACF Health Checks.

IRRH201I  The RACF_GRS_RNL check cannot be executed in a GRS=NONE environment.

Explanation: The RACF check RACF_GRS_RNL is not applicable to a GRS=NONE environment.

System action: The check stops processing. There is no effect on the system.

Operator response: Report this problem to the system programmer.

System programmer response: Disable the RACF_GRS_RNL RACF check.

Problem Determination:


See z/OS MVS Planning: Global Resource Serialization.

Automation: N/A

Detecting Module: IRRHCR00

Routing Code: N/A

Descriptor Code: N/A

IRRH202E One or more RACF ENQ names were found in a GRS Resource Name List.

Explanation: The RACF RACF_GRS_RNL check has detected that a RACF resource is covered by an entry in the specified GRS Resource Name List (RNL). RACF resource names should not be in either the system inclusion RNL (SIRNL) or the system exclusion RNL (SERNL).

System action: The check continues processing. There is no effect on the system.

Operator response: Report this problem to the system programmer.

System programmer response: Ensure that the RACF resource names are removed from the specified resource name list (RNL).

Problem Determination: See z/OS MVS Planning: Global Resource Serialization for details on resource name lists (RNLs). Ensure that the RACF ENQ names do not match any of your resource name list entries. A list of the RACF ENQ names might be found in z/OS Security Server RACF System Programmer’s Guide.


See z/OS MVS Planning: Global Resource Serialization.

Automation: N/A

Detecting Module: IRRHCR00

Routing Code: N/A

Descriptor Code: N/A
IRRH203I  No RACF ENQ names were found in the GRS Resource Name List.

**Explanation:** The RACF RACF_GRS_RNL check has not detected a conflict between the GRS Resource Name Lists (RNLs) and the RACF ENQ names.

**System action:** The check continues processing. There is no effect on the system.

**Operator response:** None.

**System programmer response:** None.

**Problem Determination:** None.

**Source:** See z/OS Security Server RACF System Programmer’s Guide.

**Reference Documentation:** See z/OS Security Server RACF System Programmer’s Guide.

See z/OS MVS Planning: Global Resource Serialization.

**Automation:** N/A

**Detecting Module:** IRRHCR00

**Routing Code:** N/A

**Descriptor Code:** N/A

---

IRRH204E  The RACF_SENSITIVE_RESOURCES check has found one or more potential errors in the security controls on this system.

**Explanation:** The RACF security configuration check has found one or more potential errors with the system protection mechanisms.

**System action:** The check continues processing. There is no effect on the system.

**Operator response:** Report this problem to the system security administrator and the system auditor.

**System programmer response:** Examine the report that was produced by the RACF check. Any resource that has an "E" in the "S" (Status) column has excessive authority allowed to the resource. This authority might come from a universal access (UACC) or ID(*) access list entry that is too permissive, or the profile is in WARNING mode. If there is no profile, PROTECTALL(FAIL) is not in effect. If the resource is a data set and there is a "V" in the "S" (Status) field, the data set is not on the indicated volume. If this data set is not an SMS data set, it might have been migrated. Remove these data sets from the list or allocate the data sets on the volume. Any data set that has an "M" in the "S" (Status) field has been migrated. Any data set that has a "U" in the "S" (Status) field has not been checked, because the data set was in use by another user.

The CSV_APF_EXISTS check provides additional analysis of the non-RACF aspects of your APF list.

If the "S" field contains an "E" or is blank, blanks in the UACC, WARN, and ID(*) columns indicate that there is no RACF profile protecting the data set. Data sets that do not have a RACF profile are flagged as exceptions, unless SETROPTS PROTECTALL(FAIL) is in effect for the system.

If a valid user ID was specified as a parameter to the check, the user's authority to the resource is checked. If the user has an excessive authority to the resource, this authority is indicated in the USER column. For example, if the user has ALTER authority to an APF-authorized data set, the USER column contains ">Read" to indicate that the user has more than READ authority to the data set.

Modules which are flagged in the ICHAUTAB report as exceptions must be either removed from ICHAUTAB or the module must be moved to a non-LPA location and the module protected by using Program Control. The users of this module should be limited to only those who are trusted to execute the program in the expected manner.

**Note:** A volume serial of "******" for any data set indicates a possible problem with the volume. Run the check in DEBUG mode, which will cause HZSDSINF to report any of its exception messages.


**Source:** See z/OS Security Server RACF Auditor’s Guide
The RACF_SENSITIVE_RESOURCES check has not found any errors in the security controls on this system.

Explanation: The RACF_SENSITIVE_RESOURCES check has not found any errors in the security controls on this system.

System action: The check continues processing. There is no effect on the system.

Operator response: None.

System programmer response: None.

Problem Determination:

Source:

Reference Documentation: None.

Automation: N/A

Detecting Module: IRRHCR00

Routing Code: N/A

Descriptor Code: N/A

The RACF_GRS_RNL check does not expect any parameters.

Explanation: The installation has defined a parameter for this check. The check expects no parameters.

System action: The check continues processing. There is no effect on the system.

Operator response: None.

System programmer response: Remove the parameter.

Problem Determination:

Source:

Reference Documentation: None.

Automation: N/A

Detecting Module: IRRHCR00

Routing Code: N/A

Descriptor Code: N/A

The RACF_SENSITIVE_RESOURCES check expects only a 1 to 8 character user ID.

Explanation: The installation has defined a parameter for this check. The specified parameter must be a valid user ID.

System action: The check continues processing. There is no effect on the system.

Operator response: None.

System programmer response: Correct the parameter.

Problem Determination:
IRRH222I  The user ID "userId", which was specified as a parameter to the RACF_SENSITIVE_RESOURCES check, does not exist.

Explanation: The installation has defined a parameter for this check. The user ID that was specified as the parameter does not exist.

System action: The check continues processing. There is no effect on the system.

Operator response: None.

System programmer response: Correct the parameter.

Problem Determination:

Source:

Reference Documentation: None.

Automation: N/A

Detecting Module: IRRHCR00

Routing Code: N/A

Descriptor Code: N/A

IRRH223I  The user ID "userId", which was specified as a parameter to the RACF_SENSITIVE_RESOURCES check, is revoked.

Explanation: The installation has defined a parameter for the check. The user ID, which was specified as the parameter, is revoked.

System action: The check continues processing. There is no effect on the system.

Operator response: None.

System programmer response: Correct the parameter.

Problem Determination:

Source:

Reference Documentation: None.

Automation: N/A

Detecting Module: IRRHCR00

Routing Code: N/A

Descriptor Code: N/A

IRRH224I  The user ID IBMUSER is revoked.

Explanation: The user ID IBMUSER is revoked. This is the recommended state of IBMUSER.

System action: The check continues processing. There is no effect on the system.

Operator response: None.

System programmer response: None.
Problem Determination:
Source:
Reference Documentation: None.
Automation: N/A
Detecting Module: IRRHCR00
Routing Code: N/A
Descriptor Code: N/A

IRRH225E The user ID IBMUSER is not revoked.
Explanation: The user ID IBMUSER has not been revoked. IBM recommends revoking IBMUSER.
System action: The check continues processing. There is no effect on the system.
Operator response: Report this problem to the system security administrator and the system auditor.
System programmer response: Revoke IBMUSER.
Automation: N/A
Detecting Module: IRRHCR00
Routing Code: N/A
Descriptor Code: N/A

IRRH226I Unexpected error in the RACF_IBMUSER_REVOKED check.
Explanation: The RACF_IBMUSER_REVOKED check encountered an unexpected error.
System action: The check continues processing. There is no effect on the system.
Operator response: None.
System programmer response: None.
Problem Determination: None.
Source: None.
Reference Documentation: None.
Automation: N/A
Detecting Module: IRRHCR00
Routing Code: N/A
Descriptor Code: N/A

IRRH227I The check-name check expects only a 1 to 8 character class name.
Explanation: The installation has defined a parameter for this check. The specified parameter must be a valid class name.
System action: The check stops processing. There is no effect on the system.
Operator response: None.
System programmer response: Correct the parameter.
Problem Determination:
Source:
Reference Documentation: None.
Automation: N/A
Detecting Module: IRRHCR00
Routing Code: N/A
Descriptor Code: N/A

IRRH228I  The class class-name is active.
Explanation: The class is active. This is the recommended state of this class.
System action: The check continues processing. There is no effect on the system.
Operator response: None.
System programmer response: None.

Problem Determination:
Source:
Reference Documentation: None.
Automation: N/A
Detecting Module: IRRHCR00
Routing Code: N/A
Descriptor Code: N/A

IRRH229E  The class class-name is not active.
Explanation: The security administrator should evaluate the need for this class, define profiles in it as appropriate, and activate the class.
System action: The check continues processing. There is no effect on the system.
Operator response: Report this problem to the system security administrator and the system auditor.
System programmer response: None.

Automation: N/A
Detecting Module: IRRHCR00
Routing Code: N/A
Descriptor Code: N/A

IRRH230I  Unexpected error in the check.
Explanation: The check encountered an unexpected error.
System action: The check continues processing. There is no effect on the system.
Operator response: None.
IRRH231I The profile profile-name contains an incorrect number of separators in member member-value of the member list. The correct number of separators is 3.

Explanation: The check-name check expects a parameter that is the name of a profile in the RACFHC class which contains the list of resources that the check is to examine. The profile name which was specified in the check has a member list, but that member list is in error. The format of the member list entry is: ADDMEM(class/resource_name/volume/NONE|READ|UPDATE|CONTROL). One of the following errors occurred:

- The class does not exist.
- The length of the resource name does not match the maximum value allowed for the class.
- A volume serial was specified for a class other than data set.
- The maximum "general user" access level specified a value other than 'NONE', 'READ', 'UPDATE', or 'CONTROL'.
- A special resource list name of other than 'IRR_APFLIST', 'IRR_LINKLIST', 'IRR_PARMLIB', 'IRR_RACFDB', 'IRR_ICHAUTAB', or 'IRR_SYSREXX' was specified. If one of these special resource names was specified no other value may be specified in the member list entry.

System action: The check scans the remaining ADDMEM entries and raises the parameter error condition. There is no effect on the system.

Operator response: None.

System programmer response: None.

Problem Determination:

Source:

Reference Documentation: None.

Automation: N/A

Detecting Module: IRRHCR00

Routing Code: N/A

Descriptor Code: N/A

IRRH232I The profile profile-name does not exist in the RACFHC class.

Explanation: The check-name check expects a parameter that is the name of a profile in the RACFHC class which contains the list of resources that the check is to examine. The profile name which was specified in the check parameter does not exist in the RACFHC class.

System action: The check stops processing and raises the parameter error condition. There is no effect on the system.

Operator response: None.

System programmer response: Change the parameter to an existing profile name in the RACFHC class which contains the list of resources that the check is to examine and rerun the check.

Problem Determination:

Source:
**IRRH233I**  The profile *profile-name* does not have any resources in the member list.

**Explanation:** The *check-name* check expects a parameter that is the name of a profile in the RACFHC class which contains the list of resources that the check is to examine. The profile name which was specified in the check does not contain a list of resources.

**System action:** The check stops processing and raises the parameter error condition. There is no effect on the system.

**Operator response:** None.

**System programmer response:** Change the parameter to an existing profile name in the RACFHC class which contains the list of resources that the check or alter the specified profile by using RALTER RACFHC *profile-name* ADDMEM(list-of-resources) to add the resources which are to be checked and rerun the check.

**Problem Determination:**

**Source:**


Automation: None.

Detecting Module: IRRHCR00

Routing Code:

Descriptor Code:

---

**IRRH234I**  The profile *profile-name* has an error in member member-number of the member list.

**Explanation:** The *check-name* check expects a parameter that is the name of a profile in the RACFHC class which contains the list of resources that the check is to examine. The profile name which was specified in the check has a member list, but that member list is in error. The format of the member list entry is: ADDMEM(class/resource_name/volume/NONE|READ|UPDATE|ALTER). One of the following errors occurred:

- The class does not exist.
- The length of the resource name does not match the maximum value allowed for the class.
- A volume serial was specified for a class other than data set.
- The maximum “general user” access level specified a value other than: ‘NONE’, ‘READ’, ‘UPDATE’, or ‘ALTER’.
- A special resource list name specified a value other than ‘IRR_APFLIST’, ‘IRR_LINKLIST’, ‘IRR_PARMLIB’, ‘IRR_RACFDB’, ‘IRR_ICHAUTAB’, or ‘IRR_SYSREXX’ was specified.

**System action:** The check stops processing and raises the parameter error condition. There is no effect on the system.

**Operator response:** None.

**System programmer response:** Change the parameter to an existing profile name in the RACFHC class which contains the list of resources that the check or alter the specified profile by using RALTER RACFHC *profile-name* command to delete the erroneous entry or entries and rerun the check.

**Problem Determination:**

**Source:**

Automation: None.
Detecting Module: IRRHCR00
Routing Code:
Descriptor Code:

IRRH2351 RACF is temporarily inactive.

Explanation: The check-name check has determined that RACF is temporarily inactive.

System action: The check stops processing. The check is eligible to run at the next interval. There is no effect on the system.

Operator response: None.
System programmer response: Determine why RACF is inactive. When RACF is made active again, the check can be run again.

Problem Determination:
Source:


Automation: None.
Detecting Module: IRRHCR00
Routing Code:
Descriptor Code:

IRRH237E The check-name check has found one or more potential errors in the security controls for the resources specified in this check.

Explanation: The RACF security configuration check has found one or more potential errors with the protection mechanisms for the resources specified for this check.

System action: The check continues processing. There is no effect on the system.

Operator response: Report this problem to your system security administrator and your system auditor.
System programmer response: Examine the report that was produced by the check. Any resource which has an "E" in the "S" (Status) column has excessive authority allowed to the resource. That authority may come from a universal access (UACC) or ID(*) access list entry which is too permissive, or if the profile is in WARNING mode. If the resource is a data set and there is no profile, then PROTECTALL(FAIL) is not in effect. Any data set which has a "V" in the "S" (Status) field is not on the indicated volume. Remove these data sets from the list or allocate the data sets on the volume. Any data set which has an "M" in the "S" (Status) field has been migrated. If the "S" field contains an "E" or is blank, then blanks in the UACC, WARN, and ID(*) columns indicate that there is no RACF profile protecting the resource. Resources which do not have a RACF profile are flagged as exceptions, unless the resource is a data set and SETROPTS PROTECTALL(FAIL) is in effect for the system.

If a valid user ID was specified as a parameter to the check, that user's authority to the resource is checked. If the user has an excessive authority to the resource, that is indicated in the USER column.

Modules which are flagged in the ICHAUTAB report as exceptions must be either removed from ICHAUTAB or the module must be moved to a non-LPA location and the module protected by using Program Control. The users of this module should be limited to only those who are trusted to execute the program in the expected manner.

Problem Determination: None.
Source:
Reference Documentation: None.
The check-name check has not found any errors in the security controls for the installation-specified resources.

Explanation: The check-name check has not found any errors in the security controls for the installation-specified resources that are specified for review by this check.

System action: The check continues processing. There is no effect on the system.

Operator response: None.

System programmer response: None.

Problem Determination: None.

Source: Reference Documentation: None.

There are no ICHAUTAB programs on this system.

Explanation: The check-name check has determined that there are no ICHAUTAB programs on this system.

System action: The check continues processing. There is no effect on the system.

Operator response: None.

System programmer response: None.

Problem Determination: None.


The check-name check has found one or more non-LPA ICHAUTAB entries.

Explanation: The check-name check has found one or more non-LPA ICHAUTAB entries. IBM recommends that ICHAUTAB contain no entries. An entry in ICHAUTAB represents a program whose access should be controlled by using PROGRAM CONTROL and restricted to a known set of trusted users or trusted started tasks. LPA-resident ICHAUTAB entries are listed in the RACF_SENSITIVE_RESOURCES check.

System action: The check continues processing. There is no effect on the system.

Operator response: None.

System programmer response: If the modules in ICHAUTAB are no longer in use, they should be deleted from ICHAUTAB. If the modules are still in use and the privileges granted by ICHAUTAB are still required, the modules
should be protected by using PROGRAM CONTROL and their use should be restricted to a known set of trusted users or trusted started tasks.

Problem Determination:

Source:


Automation: None.

Detecting Module: IRRHCR00

Routing Code:

Descriptor Code:

IRRH500I The RACF database is at the suggested stage of application identity mapping (AIM). The database is at AIM stage 03.

Explanation: The RACF_AIM_STAGE check has determined that the RACF database is at the suggested stage of application identity mapping (AIM).

System action: The check continues processing. There is no effect on the system.

Operator response: None.

System programmer response: None.

Problem Determination: None.

Source:

Reference Documentation: None.

Automation: None.

Detecting Module: IRRHCR00

Routing Code:

Descriptor Code:

IRRH500E The RACF database is not at the suggested stage of application identity mapping (AIM). The database is at AIM stage AIM-stage.

Explanation: The RACF_AIM_STAGE check has determined that the RACF database is not at the suggested stage of application identity mapping (AIM). Your system programmer can convert your RACF database using the IRRIRA00 conversion utility. See z/OS Security Server RACF System Programmer’s Guide for information about running the IRRIRA00 conversion utility.

Stage 3 of application identity mapping allows RACF to more efficiently handle authentication and authorization requests from applications such as z/OS UNIX and is required to use some RACF function. You should assign a unique UNIX UID for each user and a unique GID for each group that needs access to z/OS UNIX functions and resources. Assigning unique IDs rather than shared IDs improves overall security and increases user accountability. However, if you have a large number of users without OMVS segments who need access to z/OS UNIX services, such as FTP, you might choose not to assign UNIX identities in advance of their need to use the services. In these cases, when your RACF database has been converted to AIM stage 3, you can enable RACF to automatically assign unique UNIX UIDs and GIDs at the time they are needed. See z/OS Security Server RACF Security Administrator’s Guide for information about enabling RACF for automatic assignment of unique UNIX identities.

System action: The check continues processing. There is no effect on the system.

Operator response: Report this problem to the system security administrator.

System programmer response: If you want to use RACF function such as support for automatically assigning unique UNIX UIDs and GIDs at the time that they are needed, run the IRRIRA00 utility to advance the RACF database to application identity mapping stage 3. For details about using the IRRIRA00 utility, see z/OS Security Server RACF System Programmer’s Guide.
Problem Determination:


Reference Documentation:

Automation: None.

Detecting Module: IRRHCR10

Routing Code:

Descriptor Code:

IRRH502I RACF attempts to assign unique UNIX IDs when users or groups that do not have OMVS segments use certain z/OS UNIX services.

Explanation: The RACF UNIX identity check has determined that you want RACF to assign unique UNIX IDs when users or groups without OMVS segments use certain z/OS UNIX services. Assigning unique UNIX identities rather than shared identities improves overall security and increases user accountability.

RACF automatically assigns unique UNIX identities for z/OS UNIX services when all of the following requirements are satisfied:

1. The RACF database is enabled for application identity mapping (AIM) stage 3.
2. The UNIXPRIV class profile SHARED.IDS is defined and the UNIXPRIV class is active and RACLISTed.
3. The FACILITY class profile BPX.NEXT.USER is defined and its APPLDATA field has valid ID values or ranges.
4. The FACILITY class profile BPX.UNIQUE.USER is defined.


The check produces a report listing the requirements for this support. An "E" in the "S" (Status) column indicates that a requirement is not satisfied. For example, if the RACF database has not been enabled for AIM stage 3, this requirement is flagged as an exception. If the "S" field is blank, the requirement is satisfied. If there are no exceptions indicated in the Status column, all requirements are satisfied.

Note: The check validates that the FACILITY class profile BPX.NEXT.USER APPLDATA field is present, not that it has valid ID values or ranges.

System action: The check continues processing. There is no effect on the system.

Operator response: None.

System programmer response: None.

Problem Determination:


Reference Documentation:

Automation: None.

Detecting Module: IRRHCR10

Routing Code:

Descriptor Code:

IRRH503E RACF cannot assign unique UNIX IDs when users or groups that do not have OMVS segments use certain z/OS UNIX services. One or more requirements are not satisfied.

Explanation: The RACF UNIX identity check has determined that you want RACF to assign unique UNIX IDs when users or groups without OMVS segments use certain z/OS UNIX services. However, RACF is not able to assign unique UNIX identities for z/OS UNIX services because one or more of the following requirements are not satisfied:

1. The RACF database is enabled for application identity mapping (AIM) stage 3.
2. The UNIXPRIV class profile SHARED.IDS is defined and the UNIXPRIV class is active and RACLISTed.
3. The FACILITY class profile BPX.NEXT.USER is defined and its APPLDATA field has valid ID values or ranges.
4. The FACILITY class profile BPX.UNIQUE.USER is defined.


**System action:** The check continues processing. There is no effect on the system.

**Operator response:** Report this problem to the system security administrator.

**System programmer response:** None.

**Problem Determination:** The check produces a report listing the requirements. An "E" in the "S" (Status) column indicates that a requirement is not satisfied. For example, if the RACF database has not been enabled for AIM stage 3, this requirement is flagged as an exception. If the "S" field is blank, the requirement is satisfied. One or more requirements are not satisfied and have been flagged as an exception in the Status column.

**Source:**


**Automation:** None.

**Detecting Module:** IRRHCR10

**Routing Code:**

**Descriptor Code:**

---

**IRRH504I** RACF is not enabled to assign UNIX IDs when users or groups that do not have OMVS segments use certain z/OS UNIX services. If you choose not to define UNIX IDs for each user of UNIX functions, you can enable RACF to automatically generate unique UNIX UIDs and GIDs for you.

**Explanation:** The RACF UNIX identity check has determined that RACF is not enabled to assign UNIX IDs when users or groups that do not have OMVS segments use certain z/OS UNIX services. Users and groups that need to access z/OS UNIX functions and resources should be assigned unique UNIX UIDs and unique GIDs in advance of their need to access these services.

However, if you have a large number of users without OMVS segments that need access to z/OS UNIX services, such as FTP, you might choose not to assign UNIX identities in advance. In these cases, you can enable RACF to automatically assign unique UIDs and GIDs at the time they are needed—when users without OMVS segments access certain z/OS UNIX services.

RACF automatically assigns unique identities for z/OS UNIX services when all of the following requirements are satisfied:
1. The RACF database is enabled for application identity mapping (AIM) stage 3.
2. The UNIXPRIV class profile SHARED.IDS is defined and the UNIXPRIV class is active and RACLISTed.
3. The FACILITY class profile BPX.NEXT.USER is defined and its APPLDATA field has valid ID values or ranges.
4. The FACILITY class profile BPX.UNIQUE.USER is defined.

However, the FACILITY class profile BPX.UNIQUE.USER is not defined, so RACF is not enabled to automatically assign unique UNIX identities for z/OS UNIX services. If you would like to use this support, see [z/OS Security Server RACF Security Administrator's Guide](https://publib.boulder.ibm.com/infocenter/ciczos/v1r8/topic/sg247889.html) for more information.

**System action:** The check continues processing. There is no effect on the system.

**Operator response:** None.

**System programmer response:** None.

**Problem Determination:**

**Source:**


**Automation:** None.
The BPX.DEFAULT.USER profile in the FACILITY class indicates that you want RACF to assign shared default UNIX IDs when users or groups that do not have OMVS segments use certain z/OS UNIX services.

Explanation: The RACF UNIX identity check has found the BPX.DEFAULT.USER profile in the FACILITY class. The presence of this profile indicates an intent to have RACF assign shared default UNIX UIDs and GIDs when users without OMVS segments access the system to use certain UNIX services.

On z/OS V1R13 and below, you have the option of enabling RACF to assign default z/OS UNIX identities, however it is not suggested. You should either define OMVS segments for user and group profiles, with unique UIDs and GIDs, or you should enable RACF to automatically assign unique z/OS UNIX identities when users without OMVS segments access the system to use certain UNIX services. Assigning unique identities rather than shared identities improves overall security and increases user accountability.

Note: z/OS V1R13 is the last release that supports default UNIX identities. After z/OS V1R13, users and groups that need to access z/OS UNIX functions and resources must be assigned unique UNIX UIDs and unique GIDs in advance of their need to access these services, or you must enable RACF to automatically assign unique UNIX identities when users without OMVS segments access the system to use certain UNIX services. The FACILITY class BPX.DEFAULT.USER profile is no longer used and can be deleted.

System action: The check continues processing. There is no effect on the system.

Operator response: Report this problem to the system security administrator.

System programmer response: None.

Problem Determination:

Source:

Reference Documentation: See z/OS Security Server RACF Security Administrator's Guide for more information about how to assign a user identifier (UID) to a RACF user and how to assign a group identifier (GID) to a RACF group. RACF Security Administrator’s Guide also contains information about how to enable RACF to automatically assign unique UNIX identities.

Automation: None.

Detecting Module: IRRHCR10
Routing Code: IRRHCR0
Descriptor Code: IRRH505E

The RACF UNIX identity check has detected no exceptions.

Explanation: The RACF UNIX identity check has examined the requirements for enabling RACF to assign unique UNIX IDs when users or groups without OMVS segments use certain z/OS UNIX services. No exceptions have been detected.

System action: The check continues processing. There is no effect on the system.

Operator response: None.

System programmer response: None.

Problem Determination:

Source:

Reference Documentation: None.

Automation: None.
**IRRH507I** RACF cannot assign unique UNIX IDs when users or groups that do not have OMVS segments use certain z/OS UNIX services. One or more requirements are not satisfied.

**Explanation:** The RACF UNIX identity migration check has determined that you want RACF to assign unique UNIX IDs when users or groups without OMVS segments use certain z/OS UNIX services. However, RACF is not able to do this because one or more requirements are not satisfied.

No migration actions are required because enabling RACF to automatically assign unique z/OS UNIX identities is the recommended alternative to assigning unique UNIX UIDs and unique GIDs to users and groups in advance of their need to access z/OS UNIX functions. However, if you wish to use this support, you should examine the list of requirements and ensure that they are satisfied:

1. The RACF database is enabled for application identity mapping (AIM) stage 3.
2. The UNIXPRIV class profile SHARED.IDS is defined and the UNIXPRIV class is active and RACLISTed.
3. The FACILITY class profile BPX.NEXT.USER is defined and its APPLDATA field has valid ID values or ranges.
4. The FACILITY class profile BPX.UNIQUE.USER is defined.

See **z/OS Security Server RACF Security Administrator’s Guide** or more information about enabling RACF for automatic assignment of unique UNIX identities.

The check produces a report listing the requirements. An "E" in the "S" (Status) column indicates that a requirement is not satisfied. For example, if the RACF database has not been enabled for AIM stage 3, this requirement is flagged as an exception. If the "S" field is blank, the requirement is satisfied. One or more requirements are not satisfied and have been flagged as an exception in the Status column.

**System action:** The check continues processing. There is no effect on the system.

**Operator response:** Report this problem to the system security administrator.

**System programmer response:** None.

**Problem Determination:** None.

**Source:**

**Reference Documentation:** See **z/OS Security Server RACF Security Administrator’s Guide**

**Automation:** None.

**Detecting Module:** IRRHCR10

**Routing Code:**

**Descriptor Code:**
For more information about Health check messages, see **IBM Health Checker for z/OS: User’s Guide**
Chapter 9. SAF user mapping plug-in related messages

This chapter lists messages that are C error strings returned to the calling application. The calling application can choose to display the messages on the console or log them elsewhere. All strings are NULL terminated. The format of these error strings is:

```
IRRPInnnI text
```

where:

- **IRR** identifies the message as a RACF message.
- **PI** identifies the message as a message from the SAF plug-in.
- **nnn** is the serial number of the message. Message ids in the range 000 - 099 are returned by the SAF user mapping plug-in dll, irrspim. Message ids in the range 100 - 199 are returned by the default implementation of the SAF user mapping plug-in (irrspime).
- **text** is the text of the message.

---

**IRRPI000I**  SAF user mapping plug-in service is successful.

**Explanation:** The SAF user mapping plug-in function worked normally.

**System action:** None.

**IRRPI002I** Parameter SafmapHandle in function safMappingInit() is missing or incorrect.

**Explanation:** The safMappingInit() function requires a parameter of type SafmapHandle. The parameter was not specified (that is, NULL), or it was not initialized to X'00'.

**System action:** The SAF user mapping plug-in function processing ends. The request is not completed.

**Application Programmer Response:** Update the SafmapHandle parameter on the call to the safMappingInit() function, then try the request again.

---

**IRRPI003I** safMappingInit() is unable to open dll dllName

**Explanation:** The safMappingInit() function attempted to open the dll irrspime or the specified dll using the dlopen() service and it failed.

**System action:** The SAF user mapping plug-in function processing ends. The request is not completed.

**System Programmer Response:** Determine if the correct dll is being loaded. Make the necessary corrections and try the request again.

---

**IRRPI004I** safMappingInit() is unable to find the RMAPINIT symbol in dll dllName

**Explanation:** The dll that was loaded does not contain the RMAPINIT entry point.

**System action:** The SAF user mapping plug-in function processing ends. The request is not completed.

**Application Programmer Response:** Ensure that the plug-in implementation has exported the RMAPINIT symbol.

**System Programmer Response:** Determine if the correct dll is being loaded. Make the necessary corrections and try the request again.

---

**IRRPI005I** safMappingInit() is unable to find the RMAPLOOK symbol in dll dllName

**Explanation:** The dll that was loaded does not contain the RMAPLOOK entry point.

**System action:** The SAF user mapping plug-in function processing ends. The request is not completed.

**Application Programmer Response:** Ensure that the plug-in implementation has exported the RMAPLOOK symbol.

**EIM Administrator Response:** None.

**System Programmer Response:** Determine if the correct dll is being loaded. Make the necessary corrections and try the request again.

---

**IRRPI006I** safMappingInit() is unable to find the RMAPTERM symbol in dll dllName

**Explanation:** The dll that was loaded does not contain the RMAPTERM entry point.
IRRPI007I  Parameter SafmapHandle for function safMappingTerm() is missing or incorrect.

Explanation: The safMappingTerm() function requires a parameter of type SafmapHandle. The parameter was not specified (that is, NULL). This message is written to stderr.

System action: The SAF user mapping plug-in function processing ends. The request is not completed.

Application Programmer Response: Add the SafmapHandle parameter to the safMappingTerm() function, then try the request again.

IRRPI008I  Parameter SafmapHandle in function safMappingLookup() is missing or incorrect.

Explanation: The safMappingLookup() function requires a parameter of type SafmapHandle. The parameter was not specified (that is, NULL), or it was all X'00'.

System action: The SAF user mapping plug-in function processing ends. The request is not completed.

Application Programmer Response: Add the SafmapHandle parameter to the safMappingLookup() function, then try the request again.

IRRPI009I  Parameter SafmapCreds in function safMappingLookup() is missing or incorrect.

Explanation: The safMappingLookup() function requires a parameter of type SafmapCreds. The parameter was not specified (that is, NULL), or there is an error in the SAFMAP_REGISTRY_USER credentials or the SAFMAP_USER_ONLY credentials.

System action: The SAF user mapping plug-in function processing ends. The request is not completed.

Application Programmer Response: Update the SafmapCreds parameter on the call to the safMappingLookup() function, then try the request again.

IRRPI010I  Parameter SafmapResult in function safMappingLookup() is missing or incorrect.

Explanation: The safMappingLookup() function requires a parameter of type SafmapResult. The parameter was not specified (that is, NULL).

System action: The SAF user mapping plug-in function processing ends. The request is not completed.

Application Programmer Response: Update the SafmapResult parameter on the call to the safMappingLookup() function, then try the request again.

IRRPI013I  The SAF user mapping plug-in implementation DLL could not be closed by dlclose().

Explanation: An error occurred during the processing of the safMappingTerm() function when it attempted to close the dll that the safMappingInit() function opened.

System action: The SAF user mapping plug-in function processing ends. The request is completed.

RACF Security Administrator Response: Verify that the user mapping plug-in implementation is still in the system search order or the LIBPATH of the z/OS UNIX System Services. Restore the plug-in dll to its library or directory, then try the request again.

System Programmer Response: Verify that the dll setup has not changed since the dll was opened, then try the request again.

IRRPI014I  No mapping to a SAF user ID is returned.

Explanation: The safMappingLookup() function used the SAF user mapping plug-in implementation to find a mapping from the source user credentials (SafmapCreds parameter) and optional application data (aData parameter) to a z/OS user ID stored in a user mapping repository. During the mapping lookup, either a z/OS user ID was not found, or the length of the user ID was longer than 8 characters.

System action: The SAF user mapping plug-in function processing ends. The request is completed.

Application Programmer Response: None.

Calling Application Administrator Response: Verify that the source user credentials are the required credentials, then try the request again.

EIM Administrator Response: If the default plug-in implementation is being used (irrspime), the administrator should verify that there is a mapping or policy that will return a z/OS user ID given the source
user credentials. Check that the application data required by the calling application is specified with the target EIM user ID. If another plug-in implementation is being used, consult the administrator for that plug-in's repository.

**IRRPI015I** One SAF user ID is returned.

**Explanation:** The safMappingLookup() function was able to find a z/OS user ID from the source user credentials (SafmapCreds parameter) and optional application data (aData parameter).

**System action:** The SAF user mapping plug-in function processing ends. The request is completed.

**IRRPI016I** Many SAF user IDs found. None are returned.

**Explanation:** The safMappingLookup() function used the SAF user mapping plug-in implementation to find a mapping from the source user credentials (SafmapCreds parameter) and optional application data (aData parameter) to a z/OS user ID stored in a user mapping repository. More than one z/OS user ID was found that has a mapping from the source user credentials.

**System action:** The SAF user mapping plug-in function processing ends. The completed request found more than one user credential mapping.

**Calling Application Administrator Response:** Verify that the source user credentials are the required credentials and the optional application data (aData parameter) is correct. Try the request again.

**IRRPI017I** The plug-in implementation detected a dropped connection.

**Explanation:** The lookup function in the SAF user mapping plug-in implementation lost the connection with its store of mappings between user IDs.

**System action:** The SAF user mapping plug-in function processing ends. The request is not completed.

**Application Programmer Response:** Re-initialize the plug-in and try the lookup again. If that does not resolve the problem, check the availability of the network and the data store.

**EIM Administrator Response:** Review the return values and messages from the SafmapErr structure, which is defined in the irrspim.h header file. Then correct the problem, and try the service again.

**IRRPI018I** A SAF user mapping plug-in service returned a warning.

**Explanation:** The SAF user mapping plug-in returned a nonzero SAF reason code that does not require the connection to the plug-in to be re-initialized. The safMappingLookup() service might return a warning code in any of the following situations:

- No user mapping is found for the source user credentials.
- A user ID is found, but it is too long for a z/OS user ID.
- Too many user IDs are found.

**System action:** The SAF user mapping plug-in function processing ends. The request is completed.

**EIM Administrator Response:** If the default user mapping plug-in implementation is used, verify that the mapping information for the source user credentials is correct. If another plug-in implementation is used, consult the documentation for the plug-in for the appropriate response.

**IRRPI019I** A SAF user mapping plug-in service returned an error.

**Explanation:** The SAF user mapping plug-in returned a nonzero SAF reason code that requires the connection to the plug-in to be re-initialized; for example, the plug-in implementation detected that it lost its connection with its data source.

**System action:** The SAF user mapping plug-in function processing ends. The request is not completed.

**Application Programmer Response:** The application should try to reestablish the connection.

**IRRPI020I** A SAF user mapping plug-in service returned a severe error.

**Explanation:** The SAF user mapping plug-in returned a nonzero SAF reason code that requires corrections to the configuration of the plug-in interface, a setup problem, a parameter list error, or an internal error.

**System action:** The SAF user mapping plug-in function processing ends. The request is not completed.

**RACF Security Administrator Response:** Review the return values and messages from the SafmapErr structure, which is defined in the irrspim.h header file. Then correct the problem, and try the service again.

**IRRPI100I** Parameter SafmapHandle in function safMappingLookup() is corrupted.

**Explanation:** The plug-in implementation detected a problem with the plug-in specific data that it received as part of the SafmapHandle.

**System action:** The SAF user mapping plug-in function processing ends. The request is not completed.

**Application Programmer Response:** Isolate the problem that caused the changes to the SafmapHandle parameter. Try the request again.
IRRPI101I  Parameter SafmapHandle in function safMappingTerm() is corrupted.
Explanation: The plug-in implementation detected a problem with the plug-in specific data that it received as part of the SafmapHandle.
System action: The SAF user mapping plug-in function processing ends. The request is not completed.
Application Programmer Response: Isolate the problem that caused the changes to the SafmapHandle parameter. Try the request again.

IRRPI102I eimRetrieveConfiguration() returned an error.
Explanation: The default SAF user mapping plug-in implementation searches the EIM domain for its user mappings. One of the EIM services returned an error. The error string follows this message.
System action: The SAF user mapping plug-in function processing ends. The request is not completed.
Applicaiton Programmer Response: Review the EIM error message, correct the problem, and try the request again.

IRRPI103I The mapped user ID retrieved from the EIM domain is longer than 8 characters. The user ID is userid
Explanation: The SAF user ID returned by the eimGetTargetFromSource() function is longer than 8 characters.
System action: The SAF user mapping plug-in function processing ends. The request is completed.
EIM Administrator Response: Correct the source user mapping in the EIM domain and try the request again. The user ID portion of the mapped credential must be 8 characters or less.

IRRPI104I The default SAF user mapping plug-in implementation is unable to obtain storage.
Explanation: The default plug-in implementation cannot obtain more storage.
System action: The SAF user mapping plug-in function processing ends. The request is not completed.
System Programmer Response: Increase the size of the address space used by the application and try the request again.

IRRPI105I No mapped user ID is found in the EIM domain.
Explanation: The eimGetTargetFromSource() function did not find a mapping from the source user credentials to a z/OS user ID.
System action: The SAF user mapping plug-in function processing ends. The request is completed.
EIM Administrator Response: Update the EIM domain with the intended user mapping if appropriate. Try the request again.

IRRPI106I One mapped user ID is returned from the EIM domain. The user ID is userid
Explanation: The eimGetTargetFromSource() function returned one mapping from the source user credentials to a z/OS user ID.
System action: The SAF user mapping plug-in function processing ends. The request is successfully completed.

IRRPI107I More than one mapped user ID are found in the EIM domain. The first user ID is userid
Explanation: The eimGetTargetFromSource() function found more than one mapping to a z/OS user ID from the source user credentials.
System action: The SAF user mapping plug-in function processing ends. The request is completed.
EIM Administrator Response: Correct the mappings stored in the EIM domain if appropriate. Try the request again.

IRRPI108I The credential type in the SafmapCreds parameter is not supported by the default plug-in implementation.
Explanation: The credential type in the source user credential is not supported by the default SAF user mapping plug-in implementation.
System action: The SAF user mapping plug-in function processing ends. The request is not completed.

IRRPI109I The credential type in the SafmapResult parameter is not supported by the default plug-in implementation.
Explanation: The credential type in the mapping result is not supported by the default SAF user mapping plug-in implementation.
System action: The SAF user mapping plug-in function processing ends. The request is not completed.
Application Programmer Response: Change the mapping result credential to a supported type.
IRRPI110I  eimCreateHandle() returned an error.

Explanation:  The eimCreateHandle() API used by the default plug-in implementation returned an error.

System action:  The SAF user mapping plug-in function processing ends. The request is not completed.

EIM Administrator Response:  Review the values, return codes, and messages returned in the SafmapErr structure, which is defined in the irrspim.h header file. Then correct the setup, and try the request again.

IRRPI111I  eimConnect() returned an error.

Explanation:  The eimConnect() API used by the default plug-in implementation returned an error.

System action:  The SAF user mapping plug-in function processing ends. The request is not completed.

EIM Administrator Response:  Review the values, return codes, and messages returned in the SafmapErr structure, which is defined in the irrspim.h header file. Then correct the setup, and try the request again.

IRRPI112I  eimGetTargetFromSource() returned an error.

Explanation:  The eimGetTargetFromSource() API used by the default plug-in implementation returned an error.

System action:  The SAF user mapping plug-in function processing ends. The request is not completed.

EIM Administrator Response:  Review the values, return codes, and messages returned in the SafmapErr structure, which is defined in the irrspim.h header file. Then correct the setup, and try the request again.

IRRPI113I  eimDestroyHandle() returned an error.

Explanation:  The eimDestroyHandle() API used by the default plug-in implementation returned an error.

System action:  The SAF user mapping plug-in function processing ends. The request is not completed.

EIM Administrator Response:  Review the values, return codes, and messages returned in the SafmapErr structure, which is defined in the irrspim.h header file. Then correct the setup, and try the request again.

IRRPI114I  The SAF user mapping plug-in service was successful.

Explanation:  The default user mapping plug-in implementation successfully completed the request.

System action:  The SAF user mapping plug-in function processing ends. The request is completed normally.

IRRPI115I  The bytesAvailable field value in the SafmapResult parameter is not large enough to contain user ID userid

Explanation:  The length of the user ID returned by the mapping service is too long to fit in the SafmapResult parameter.

System action:  The SAF user mapping plug-in function processing ends. The request is completed normally. No user ID is returned. The user ID in the error message might be truncated if it is too long for the SafmapError message array.

Application Programmer Response:  Increase the value in the bytes available field in the SafmapResult parameter.

IRRPI116I  The credential CCSID field in the SafmapCreds parameter is not supported by the default plug-in implementation.

Explanation:  The default plug-in implementation only supports a CCSID of IBM-1047. The credential CCSID field in the SafmapCreds parameter contains another value.

System action:  The SAF user mapping plug-in function processing ends. No user ID is returned.

Application Programmer Response:  Convert the credential to IBM-1047 before calling the safMappingLookup() function, when the safMappingLookup() function is configured to use the default plug-in implementation.

IRRPI117I  The credential CCSID field in the SafmapResult parameter is not supported by the default plug-in implementation.

Explanation:  The default plug-in implementation only supports a CCSID of IBM-1047. The credential CCSID field in the SafmapResult parameter contains another value.

System action:  The SAF user mapping plug-in function processing ends. No user ID is returned.

Application Programmer Response:  Convert the credential from IBM-1047 to the application CCSID after calling the safMappingLookup() function, when the safMappingLookup() function is configured to use the default plug-in implementation.
Chapter 10. IKJ messages

RACF commands were originally TSO commands. (TSO, or Time Sharing Option, is the means by which interactive users gain access to MVS systems.) The RACF commands are treated as TSO commands.

TSO messages (which have a prefix of IKJ) can result from syntax errors made while issuing a RACF command.

For more information on TSO IKJ messages, see z/OS TSO/E Messages.
Chapter 11. RACF abend codes

This chapter lists and explains the RACF-related abend codes that the system issues to indicate the abnormal completion of a task. Completion codes appear in hexadecimal.

182

**Explanation:** RACF cannot successfully establish an ESTAE recovery environment when processing a RACHECK request.

**System action:** The task ends.

**Problem Determination:** Register 15 contains the nonzero return code passed back from the ESTAE macro. For a description of the ESTAE return code, see z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG.

See z/OS Security Server RACF Diagnosis Guide for information about diagnosing abends and reporting abend problems to IBM.

**Note:** For batch jobs, if you need to do dump analysis but do not have a dump, run the job again. For batch jobs using DSMON, a RACF command, or the RACF report writer, specify a SYSABEND DD statement in the job. This ensures that a dump is taken.

183

**Explanation:** RACF cannot successfully establish an ESTAE recovery environment when processing a RACINIT request.

**System action:** The task ends.

**Problem Determination:** Register 15 contains the nonzero return code passed back from the ESTAE macro. For a description of the ESTAE return code, see z/OS MVS Programming: Authorized Assembler Services Reference EDT-IXG.

See z/OS Security Server RACF Diagnosis Guide for information about diagnosing abends and reporting abend problems to IBM.

**Note:** For batch jobs, if you need to do dump analysis but do not have a dump, run the job again. For batch jobs using DSMON, a RACF command, or the RACF report writer, specify a SYSABEND DD statement in the job. This will ensure that the system produces a dump.

185

**Explanation:** RACF cannot successfully establish an ESTAE recovery environment when processing a RACDEF request.

**System action:** The task ends.

**Problem Determination:** Register 15 contains the nonzero return code passed back from the ESTAE macro. For a description of the ESTAE return code, see the MVS macros and interfaces reference for your system.

See z/OS Security Server RACF Diagnosis Guide for information about diagnosing abends and reporting abend problems to IBM.

**Note:** For batch jobs, if you need to do dump analysis but do not have a dump, run the job again. For batch jobs using DSMON, a RACF command, or the RACF report writer, specify a SYSABEND DD statement in the job. This will ensure that a dump is taken.

282

**Explanation:** An error was detected by RACF in the parameters passed to RACF for RACROUTE REQUEST=AUTH processing.

**System action:** The task ends.

**Programmer response:** Register 15 contains a hexadecimal reason code (message ICH409I, if issued, also contains this reason code):

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>04</td>
<td>Parameter list length not valid.</td>
</tr>
<tr>
<td>10</td>
<td>AF authorization, or system key 0-7, or supervisor state required for CSA, LOG, PRIVATE, PROFILE, ACEE, UTOKEN, USERID, or GROUPID option.</td>
</tr>
<tr>
<td>14</td>
<td>ATTR option not valid.</td>
</tr>
<tr>
<td>18</td>
<td>Volume serial required but not supplied.</td>
</tr>
<tr>
<td>1C</td>
<td>Inconsistent PROFILE/ENTITY flag settings.</td>
</tr>
<tr>
<td>20</td>
<td>No resource name or PROFILE specified.</td>
</tr>
<tr>
<td>24</td>
<td>No CLASS name specified.</td>
</tr>
<tr>
<td>2C</td>
<td>Incorrect LOG option specified. (This code is used only through RACF Version 1.4.)</td>
</tr>
<tr>
<td>30</td>
<td>Volume serial specified for class other than DATASET.</td>
</tr>
</tbody>
</table>
34  File sequence number not valid.
38  File sequence number specified for non-tape data set.
3C  Tape label parameter specified for non-tape data set.
40  Tape label option not valid.
44  Erase-on-scratch request not valid.
48  USERID = * was specified on the REQUEST=AUTH. * is an unacceptable RACF user ID.
4C  For the ENTITYX keyword, both the entity name length and the buffer length are zero.
50  Buffer length is not valid:
      • Less than zero
      • Greater than 255
      • Not zero but less than the entity name length.
54  Entity name length is not valid:
      • Less than zero
      • Greater than 44 if CLASS=DATASET, or greater than the length for that class as defined in the class-descriptor table
      • Greater than 44 if CLASS=DATASET, or greater than the maximum length for that class as defined in the class-descriptor table.
58  The in-storage profile provided to the REQUEST=AUTH was not at the version required by RACF. Ensure that the version of the in-storage profile (addressed by the ENTITY parameter with CSA specified) is at the required version number.
5C  The entity name contains a blank.
      If the ENTITYX keyword is specified and the entity name length is given, the name has a blank in the beginning, in the middle, or at the end.
60  RTOKEN keyword is mutually exclusive with the CSA and PRIVATE parameters of the ENTITY keyword.
64  ACEE not valid.
68  Unauthorized caller specified subpool greater than 127 on RACROUTE MSGSP parameter.
6C  The message chain pointed to by SAFPMSAD for an unauthorized caller contains too many elements, indicating a chaining problem.

Identify and correct the indicated error.

Problem Determination: Use the reason code in Register 15 to identify the error. If the issuer of the RACF macro is a user routine (such as an installation exit), correct the parameter list specified for the RACF macro in the installation exit. If the issuer of the RACF macro is an IBM routine, see [z/OS Security Server RACF Diagnosis Guide](https://www.ibm.com/support/knowledgecenter/en/SSS778_13.1.0/com.ibm.zos.racf.racfdiag.doc/131r60002.html) for more information about diagnosing abends and reporting abend problems to IBM.

Note: For batch jobs, if you need to do dump analysis but do not have a dump, run the job again. For batch jobs using DSMON, a RACF command, or the RACF report writer, specify a SYSABEND DD statement in the job. This ensures that a dump is taken.

---

283

Explanation: An error was detected by RACF in the parameters passed to RACF for RACROUTE REQUEST=VERIFY processing.

System action: The task ends.

Programmer response: Register 15 contains a hexadecimal reason code. (Message ICH409I, if issued, also contains this reason code.)

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>04</td>
<td>Incorrect parameter list length.</td>
</tr>
<tr>
<td>14</td>
<td>ENVIR data specified was not valid.</td>
</tr>
<tr>
<td>18</td>
<td>USERID specified did not conform to length requirements.</td>
</tr>
<tr>
<td>1C</td>
<td>PASSWRD or PHRASE specified did not conform to length requirements.</td>
</tr>
<tr>
<td>20</td>
<td>GROUP specified did not conform to length requirements.</td>
</tr>
<tr>
<td>24</td>
<td>NEWPASS or NEWPHRASE specified did not conform to length requirements.</td>
</tr>
<tr>
<td>28</td>
<td>OIDCARD specified had length field=0.</td>
</tr>
<tr>
<td>30</td>
<td>One of the following conditions caused this error:</td>
</tr>
<tr>
<td></td>
<td>• Incorrect combination of ENVIR keyword data and USERID, PASSWRD, NESTED, NEWPASS, START, OIDCARD, TERMD, APPL, SESSION, TRUSTED, REMOTE, SECLABEL, EXENODE, SERVAUTH, SUSERID, SNODE, SGROUP, POE, POENET, TOKNIN, and STOKEN specified.</td>
</tr>
<tr>
<td></td>
<td>• PHRASE or NEWPHRASE is specified with ENVIR other than CREATE.</td>
</tr>
<tr>
<td>34</td>
<td>Incorrect combination of ENVIR keyword data and GROUP specified.</td>
</tr>
<tr>
<td>38</td>
<td>ENVIR = CHANGE specified but no ACEE exits.</td>
</tr>
<tr>
<td>3C</td>
<td>One of the following conditions caused this error:</td>
</tr>
<tr>
<td></td>
<td>• User ID specified is <em>NONE</em> and REQUEST=VERIFY is not branch entered.</td>
</tr>
</tbody>
</table>
Identify and correct the indicated error.

**Problem Determination:** Use the reason code in Register 15 to identify the error. If the issuer of the RACF macro is a user routine (such as an installation exit), correct the parameter list specified for the RACF macro in the installation exit. If the issuer of the RACF macro is an IBM routine, see z/OS Security Server RACF Diagnosis Guide for information about diagnosing abends and reporting abend problems to IBM.

**Note:** For batch jobs, if you need to do dump analysis but do not have a dump, run the job again. For batch jobs using DSMON, a RACF command, or the RACF report writer, specify a SYSABEND DD statement in the job. This will ensure that a dump is taken.

---

**Code** | **Explanation**
--- | ---
04 | Parameter list length is not valid.
08 | Level number is not valid.
0C | TYPE option is not valid.
10 | Resource name required. **Entity-name** (and **newname** keywords, if specified) must point to valid, non-blank resource names.
14 | New data set name or old volume serial specified but address is zero.
18 | Volume serial required but not specified.
1C | New data set name and old volume serial flags both set.
24 | Parameters supplied that are inconsistent for a general resource class other than DATASET. These incorrect parameters might be model name, model volume serial, VSAM data set bit on, old volume serial, or new data set name.
28 | Model resource information supplied with type other than DEFINE for DATASET class.
2C | Model name supplied but model volume serial not supplied.
30 | Unqualified data set name specified. This return code is not issued if RACFIND=NO was specified.
34 | Old volume serial number is absent for CHGVOL request.
Length of the unit field is not valid.

AUDIT value is not valid.

Specified OWNER is not valid. This reason code can occur for several reasons. Among the possible reasons are:

- The OWNER is not a RACF-defined user ID or group ID.
- The OWNER is a RACF-defined user ID but that user ID is revoked.

UACC value is not valid.

Rename request is not valid. Either ENTITY name or NEWNAME name, but not both, is a generic name. This reason code can occur because of the attempt to create a data set profile with a single-qualifier name, when RACF protection for single-qualifier names has not been activated (SETROPTS command with PREFIX specified). Note that there are several cases in which data set profiles can be created automatically: when users with the ADSP attribute create data sets, when PROTECT=YES is specified in JCL, and when a user issues the ADDSD command.

Type=CHGVOL specified for TAPE.

Parameters specified for TAPE are not valid.

FILESEQ omitted when required for TAPE.

Operands specified for DASD are not valid.

The in-storage profile provided to the RACHECK request was not at the version required by RACF. Ensure that the version of the in-storage profile (addressed by the ENTITY parameter with CSA specified) is at the required version number.

FILESEQ value is not valid.

TAPELBL value is not valid.

EXPDT/RETPD value is not valid.

NOTIFY user ID is not valid.

RESOWNER specified for other than TYPE=DEFINE.

Specified RESOWNER is not valid.

MGMTCLAS and/or STORCLAS specified without RESOWNER.

Length for MGMTCLAS is not valid.

Length for STORCLAS is not valid.

Length for RESOWNER is not valid.

Specified SECLABEL is not valid.

Buffer length specified with ENTITYX keyword is not valid:

- Greater than 255
- Not zero but less than the entity name length

Name length specified with ENTITYX keyword is not valid:

- The specified length is less than zero.
- The specified length is greater than 44 if CLASS=DATASET or greater than the maximum length for that class as defined in the class-descriptor table.
- The name that was supplied is longer than 44 if CLASS=DATASET or longer than the maximum length for that class as defined in the class-descriptor table.

For the ENTITYX format, both the entity name length and the buffer lengths are zero.

Buffer length specified with MENTX keyword is not valid:

- Less than zero
- Greater than 255
- Not zero but less than the entity name length

Name length specified with MENTX keyword is not valid:

- The specified length is less than zero.
- The specified length is greater than 44 if CLASS=DATASET or greater than the maximum length for that class as defined in the class-descriptor table.

For the MENTX keyword, both the entity name length and the buffer lengths are zero.

Buffer length specified with NEWNAMX keyword is not valid:

- Less than zero
- Greater than 255
- Not zero but less than the entity name length

Name length specified with NEWNAMX keyword is not valid:

- The specified length is less than zero.
- The specified length is greater than 44 if CLASS=DATASET or greater than the maximum length for that class as defined in the class-descriptor table.
- The name that was supplied is longer than 44 if CLASS=DATASET or longer than the maximum length for that class as defined in the class-descriptor table.

For the NEWNAMX keyword, both the entity name length and the buffer lengths are zero.

The profile name for the FILE and DIRECTRY
class does not contain at least two valid qualifiers for keyword ENTITY or ENTITYX.
- The profile name contains only one qualifier.
- The profile name begins with a period.
- The second qualifier is longer than 8 characters.

**B0**
The profile name for the FILE and DIRECTRY class does not contain at least two valid qualifiers for keyword MENTITY or MENTX.
- The profile name contains only one qualifier.
- The profile name begins with a period.
- The second qualifier is longer than 8 characters.

**B4**
The profile name for the FILE and DIRECTRY class does not contain at least two valid qualifiers for keyword NEWNAME or NEWNAMX.
- The profile name contains only one qualifier.
- The profile name begins with a period.
- The second qualifier is longer than 8 characters.

**B8**
The entity name contains a blank:
If the ENTITYX keyword is specified and the entity name length is given, the name has a blank in the beginning, in the middle, or at the end.

**BC**
The model profile name contains a blank.
If the MENTX keyword is specified and the name length is given, the name has a blank in the beginning, in the middle, or at the end.

**C0**
The new profile name contains a blank.
If the NEWNAME keyword is specified and the new name length is given, the name has a blank in the beginning, in the middle, or at the end.

**C8**
Specified SECLVL is not valid:
- The number of data fields is not zero or one.
- The value of the data fields is not within the range of 1 - 254.

Identify and correct the indicated error.

**Problem Determination:** Use the reason code in Register 15 to identify the error. If the issuer of the RACF macro is a user routine (such as an installation exit), correct the parameter list specified for the RACF macro in the installation exit. If the issuer of the RACF macro is an IBM routine, see z/OS Security Server RACF Diagnosis Guide for information about diagnosing abends and reporting abend problems to IBM.

**Note:** For batch jobs, if you need to do dump analysis but do not have a dump, run the job again. For batch jobs using DSMON, a RACF command, or the RACF report writer, specify a SYSABEND DD statement in the job. This will ensure that a dump is taken.

---

**382**

**Explanation:** The RACROUTE REQUEST=AUTH preprocessing or postprocessing exit routine passed an incorrect return code to RACF. The return code was not part of the defined interface.

**System action:** The task ends.

**Programmer response:** Possible user error. Register 15 contains the return code from the exit routine. Verify that the exit routine is issuing valid return codes. See z/OS Security Server RACROUTE Macro Reference for the correct return codes.

**Problem Determination:** If the installation exit is issuing a correct return code and RACF still issues this abend, call your IBM support center for advice about whether this is a documentation error or an incorrect output error. See z/OS Security Server RACF Diagnosis Guide for information about reporting documentation errors or incorrect output to IBM.

**Note:** Before calling IBM, make sure the return code passed by the installation exit is correct.

---

**383**

**Explanation:** The RACROUTE REQUEST=VERIFY preprocessing or postprocessing exit routine passed an incorrect return code to RACF. The return code was not part of the defined interface.

This abend occurs for an incorrect return code from the new password and new password phrase exits including the preprocessing and postprocessing exits.

**System action:** The task ends.

**Programmer response:** Possible user error. Register 15 contains the return code from the exit routine. Verify that the exit routine is issuing valid return codes. See z/OS Security Server RACROUTE Macro Reference for the correct return codes.

**Problem Determination:** If the installation exit is issuing a correct return code and RACF still issues this abend, call your IBM support center for advice about whether this is a documentation error or an incorrect output error. See z/OS Security Server RACF Diagnosis Guide for information about reporting documentation errors or incorrect output to IBM.

**Note:** Before calling IBM, make sure the return code passed by the installation exit is correct.
385

Explanation: The RACROUTE REQUEST=VERIFY preprocessing or postprocessing exit routine passed an incorrect return code to RACF. The return code was not part of the defined interface.

System action: The task ends.

Programmer response: Possible user error. Register 15 contains the return code from the exit routine. Verify that the exit routine is issuing valid return codes. See z/OS Security Server RACROUTE Macro Reference for the correct return codes.

Problem Determination: If the installation exit is issuing a correct return code and RACF still issues this abend, call your IBM support center for advice about whether this is a documentation error or an incorrect output error. See z/OS Security Server RACF Diagnosis Guide for information about reporting documentation errors or incorrect output to IBM.

Note: Before calling IBM, make sure the return code passed by the installation exit is correct.

3C7

Explanation: While RACF was processing a non-SVC request, an error occurred in the RACF storage manager.

System action: The system terminates the service request.

Programmer response: Register 15 contains a hexadecimal reason code. (Message ICH409I, if issued, also contains this reason code.)

Code | Explanation
--- | ---
04 | BAD LENGTH: The length of the area to get or free is not greater than zero.
08 | BAD ALIGNMENT: The pointer to the area to free is not on a doubleword boundary.
0C | DUPLICATE FREEMAIN: The area to free has already been freed.
10 | INCORRECT SUBPOOL: The subpool for the area to free is not the subpool in which the area is allocated.
14 | INVALID OVERLAP: Part of the area to free equals part of the area allocated, but the match is not correct for either a full or partial FREEMAIN.
18 | NOT FOUND: The area to free does not have a corresponding GETMAIN entry in the tracking table, and the caller did not specify that it should not have.
1C | FOUND: The area to free has a corresponding GETMAIN entry in the tracking table, and the caller specified that it should not have.

20 | NOT FREED: There is a temporary area still allocated at the end of processing.
A0 | A RACF module issued a get-space request. However, register 1 is not equal to zero and does not point to a buffer previously created by the program.
A4 | A RACF module issued a get-space request. However, the subpool in register 0 is not the subpool in which the previously created buffer is allocated.
A8 | A RACF module issued a free-space request. However, register 1 is equal to zero.
AC | A RACF module issued a free-space request. However, register 1 does not point to the buffer previously created by the program.

Identify and correct the indicated error.

Problem Determination: Using IPCS, format the dump taken for this abend. For an explanation of the dump title, see z/OS Security Server RACF Diagnosis Guide.

482

Explanation: While RACF was processing a RACHECK request, the RACF manager returned a return code that was not valid.

System action: The system stops the task.

Programmer response: Register 15 contains the hexadecimal return code from the RACF manager, but Register 0 does not contain the RACF manager reason code. (Message ICH409I, if issued, contains this reason code.) See "RACF manager return codes" on page 405 for an explanation of RACF-manager return codes.

Problem Determination: Using IPCS, format the dump taken for this abend. For an explanation of the dump title, see z/OS Security Server RACF Diagnosis Guide.

483

Explanation: While RACF was processing a RACINIT request, the RACF manager returned an incorrect return code.

System action: The task ends.

Programmer response: Register 15 contains the return code from the RACF manager, but Register 0 will not contain the RACF manager reason code. See "RACF manager return codes" on page 405 for an explanation of RACF-manager return codes.

Problem Determination: If a dump was taken for this abend, use IPCS, to format the dump. For an explanation of the dump title, see the dump title beginning ICHRST00-RACF SVCS in z/OS Security Server RACF Diagnosis Guide.
**485**

**Explanation:** While RACF was processing a RACROUTE REQUEST=DEFINE request, the RACF manager returned an incorrect return code.

**System action:** The task ends.

**Programmer response:** Register 15 contains the return code from the RACF manager, but Register 0 will not contain the RACF manager reason code. See "RACF manager return codes" on page 405 for an explanation for RACF-manager return codes.

**Problem Determination:** If a dump was taken for this abend, use IPCS, to format the dump. For an explanation of the dump title, see the dump title beginning **ICHRST00-RACF SVCS** in **z/OS Security Server RACF Diagnosis Guide**.

---

**4C6**

**Explanation:** An error occurred because the required control blocks were not present when a callable security service was processed. A hexadecimal reason code in register 15 describes the error. See the reason code for a description of the error.

**System action:** The system abnormally ends the task.

**Programmer response:** RACF input/output parameter list IRRPCOMP contains a SAF return code, RACF return code, and RACF reason code that describes an internal RACF error. For additional information about the parameter list IRRPCOMP, see **z/OS Security Server RACF Callable Services**.

**Code (hex) Explanation**

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>04</td>
<td>BAD LENGTH: The length of the area to get or free is not greater than zero.</td>
</tr>
<tr>
<td>08</td>
<td>BAD ALIGNMENT: The pointer to the area to free is not on a doubleword boundary.</td>
</tr>
<tr>
<td>0C</td>
<td>DUPLICATE FREEMAIN: The area to free has already been freed.</td>
</tr>
<tr>
<td>10</td>
<td>INCORRECT SUBPOOL: The subpool for the area to free is not the subpool in which the area is allocated.</td>
</tr>
<tr>
<td>14</td>
<td>INVALID OVERLAP: Part of the area to free equals part of the area allocated, but the match is not correct for either a full or partial FREEMAIN.</td>
</tr>
<tr>
<td>18</td>
<td>NOT FOUND: The area to free does not have a corresponding GETMAIN entry in the tracking table, and the caller did not specify that it should not have.</td>
</tr>
<tr>
<td>1C</td>
<td>FOUND: The area to free has a corresponding GETMAIN entry in the tracking table, and the caller specified that it should not have.</td>
</tr>
<tr>
<td>20</td>
<td>NOT FREED: There is a temporary area still allocated at the end of processing.</td>
</tr>
<tr>
<td>A0</td>
<td>A RACF module issued a get-space request. However, register 1 is not equal to zero and does not point to a buffer previously created by the program.</td>
</tr>
<tr>
<td>A4</td>
<td>A RACF module issued a get-space request. However, the subpool in register 0 is not the subpool in which the previously created buffer is allocated.</td>
</tr>
<tr>
<td>A8</td>
<td>A RACF module issued a free-space request. However, register 1 is equal to zero.</td>
</tr>
<tr>
<td>AC</td>
<td>A RACF module issued a free-space request. However, register 1 does not point to the buffer previously created by the program.</td>
</tr>
</tbody>
</table>

**Problem Determination:** Using IPCS, format the dump taken for this abend. For an explanation of the dump title, see **z/OS Security Server RACF Diagnosis Guide**. Look at the messages in the job log for the name of the module calling RACF. For modules supplied by IBM, search problem reporting databases for a fix for the problem. If no fix exists, contact the IBM support center.

---

**4C7**

**Explanation:** While RACF was processing a non-SVC request, an error occurred in the RACF storage manager.

**System action:** The task ends.
Explanation: While processing a RACROUTE REQUEST=AUTH request, RACF was unable to verify a user.

System action: The task ends.

Programmer response: Register 15 contains a hexadecimal reason code. Message ICH409I, if issued, also contains this return code.

Code Explanation

00 No accessor control environment (ACEE) was available to describe the user.
   
   Note: This is normal if a job started or a user logged on while RACF was inactive but has since been reactivated.

04 Reserved.

Identify and correct the indicated error.

Problem Determination: Run the job again, or have the user log on again while RACF is active. If the abend occurs again, see z/OS Security Server RACF Diagnosis Guide for information about diagnosing abends and reporting abend problems to IBM. For the other reason codes, correct the problem indicated by the reason code. For assistance in gathering additional information about the request that caused this abend (such as obtaining a dump or identifying the caller of RACF), see z/OS Security Server RACF Diagnosis Guide for information about diagnosing abends. If an IBM program issued the REQUEST=DEFINE macro, see z/OS Security Server RACF Diagnosis Guide for information about reporting abend problems to IBM.

Explanation: While processing a RACROUTE REQUEST=DEFINE request, RACF encountered an error.

System action: The task ends.

Programmer response: Register 15 contains a hexadecimal reason code. (Message ICH409I, if issued, also contains this return code.)

Code Explanation

00 No accessor environment element (ACEE) was available to describe the user.
   
   Note: This is normal if a job started or a user logged on while RACF was inactive but has since been reactivated.

04 No UCB was found to contain a volume serial that matched the volume serial passed to RACF in the REQUEST=DEFINE macro instruction for a TYPE=DEFINE operation.

08 The ADDVOL or CHGVOL function was requested but the user did not have at least UPDATE authority to the data set.

0C The ADDVOL function was requested and (1) the volume serial number is already defined (for DATASET class), or (2) the new tape volume is already defined (for TAPEVOL class).

The CHGVOL function was requested and a data set profile with ENTITY name and a new volume serial number is already defined.

Identify and correct the indicated error.

Problem Determination: For reason code 00, run the job again, or have the user log on again while RACF is active. If the abend occurs again, see z/OS Security Server RACF Diagnosis Guide for information about diagnosing abends and reporting abend problems to IBM. For the other reason codes, correct the problem indicated by the reason code. For assistance in gathering additional information about the request that caused this abend (such as obtaining a dump or identifying the caller of RACF), see z/OS Security Server RACF Diagnosis Guide for information about diagnosing abends. If an IBM program issued the REQUEST=DEFINE macro, see z/OS Security Server RACF Diagnosis Guide for information about reporting abend problems to IBM.

Explanation: The module calling RACROUTE REQUEST=VERIFY is not authorized (is not APF-authorized, in system key 0-7, or in supervisor state).

Note: If certain keywords are not specified on the REQUEST=VERIFY, you can authorize the calling module by entering it in the RACF-authorized caller table. See z/OS Security Server RACROUTE Macro Reference for the keywords that cannot be specified. However, you should not place entries in the RACF-authorized caller table.

System action: The task is terminated.

Programmer response: Possible user error. Verify that the module is an authorized caller.

Problem Determination: If the request originated as a RACF command (that in turn resulted in the issuing of the REQUEST=VERIFY), check to make sure the RACF command is in the list of APF-authorized commands for your system.

If the module making the request is an IBM routine, see z/OS Security Server RACF Diagnosis Guide for information about diagnosing abends and reporting abend problems to IBM.

Explanation: The module calling the RACF manager or the RACROUTE REQUEST=LIST or RACROUTE REQUEST=EXTRACT function is not authorized (is not APF-authorized, in system key 0-7, or in supervisor state).

Note: If the NEWPASS keyword is not specified on the REQUEST=VERIFY, you can authorize the calling
module by entering it in the RACF-authorized caller table. However, you should not place entries in the RACF-authorized caller table.

**System action:** The task ends.

**Programmer response:** Possible user error. Verify that the module is an authorized caller.

**Problem Determination:** If the request originated as a RACF command (that in turn resulted in a call to the RACF manager or the REQUEST=LIST), check to make sure the RACF command is in the list of APF-authorized commands for your system. Also ensure if the request was from a RACF command, the command is registered in TSO as an authorized command (in PARMLIB member IKJTSOxx under the AUTHCMD section).

If the module making the request is an IBM routine, see z/OS Security Server RACF Diagnosis Guide for information about diagnosing abends and reporting abend problems to IBM.

---

**685**

**Explanation:** The module calling RACROUTE REQUEST=DEFINE is not authorized (is not APF-authorized, in system key 0-7, or in supervisor state). To issue a REQUEST=DEFINE, the calling module must be authorized (APF-authorized, in system key 0-7, or in supervisor state).

**System action:** The task ends.

**Programmer response:** Possible user error. Verify that the calling module was executing in an authorized state.

**Problem Determination:** If the request originated as a RACF command (that in turn resulted in the issuing of the REQUEST=DEFINE), check to make sure the RACF command is in the list of APF-authorized commands for your system.

If the module making the request is an IBM routine, see z/OS Security Server RACF Diagnosis Guide for information about diagnosing abends and reporting abend problems to IBM.

---

**9C7**

**Explanation:** RACROUTE functions dealing with tokens (such as VERIFY, VERIFYX, TOKENBLD, and TOKENMAP) will issue an abend 9C7 when an incorrect parameter or token is detected.

**System action:** The task ends.

**Programmer response:** This is possibly a user error. Verify that the token interface is correct.

**Problem Determination:** Check the reason code and make sure that you pass the correct token in the request.

The following reason codes will be issued with abend 9C7.

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>STOKEN area is too small.</td>
</tr>
<tr>
<td>02</td>
<td>TOKNIN area is too small.</td>
</tr>
<tr>
<td>04</td>
<td>The request is TOKENMAP. TOKNIN is a required parameter. Either it was not specified or both its length and version fields are 0.</td>
</tr>
<tr>
<td>08</td>
<td>The request is VERIFYX, TOKENBLD, TOKENMAP, or TOKENXTR. TOKNOUT is a required parameter. Either it was not specified or both its length and version fields are 0.</td>
</tr>
<tr>
<td>0C</td>
<td>Version of 0 can only be used with a length of 0, as an alternate method of not specifying a token parameter. This token is not valid because the token’s version is 0 but its length is not.</td>
</tr>
<tr>
<td>10</td>
<td>VERSION=0.</td>
</tr>
<tr>
<td>14</td>
<td>USERID has length greater than 8 characters.</td>
</tr>
<tr>
<td>18</td>
<td>PASSWRD or PHRASE is greater than its allowed maximum.</td>
</tr>
<tr>
<td>1C</td>
<td>GROUPID has length greater than 8 characters.</td>
</tr>
<tr>
<td>20</td>
<td>NEWPASS or NEWPHRASE is greater than its allowed maximum.</td>
</tr>
<tr>
<td>24</td>
<td>EXENODE has length greater than 8 characters.</td>
</tr>
<tr>
<td>28</td>
<td>SUSERID has length greater than 8 characters.</td>
</tr>
<tr>
<td>2C</td>
<td>SNODE has length greater than 8 characters.</td>
</tr>
<tr>
<td>30</td>
<td>SGROUP has length greater than 8 characters.</td>
</tr>
<tr>
<td>34</td>
<td>TOKNOUT version is greater than the current maximum.</td>
</tr>
<tr>
<td>3C</td>
<td>User ID specified is <em>BYPASS</em> and PASSCHK=YES, if no password or password phrase is specified.</td>
</tr>
</tbody>
</table>

---

**AC5**

**Explanation:** An unexpected error was encountered during internal RACF processing for datasharing or sysplex communication functions. A hexadecimal reason code is given in register 15.

**System action:** A dump will be taken in all cases. If the abend occurs in the RACF data sharing address space, the address space will be restarted. If the abend occurs in the master address space, the system will enter failsoft mode.

**Programmer response:** The abend occurred in the master address space, the system will need to be re-IPLed in order for RACF to be made active again. If
necessary, contact your programming support personnel.

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>03</td>
<td>An error occurred when attempting to obtain storage.</td>
</tr>
<tr>
<td>05</td>
<td>An error occurred when attempting to free storage.</td>
</tr>
<tr>
<td>07</td>
<td>After IXJOIN, all other members left the data sharing group before the group data set name and range table were received. One reason this can happen is that you are IPLing a system and all other systems in the group were simultaneously re-IPLed. If this is the case, re-IPL your system. Otherwise, contact the IBM support center.</td>
</tr>
<tr>
<td>08</td>
<td>An XCF service failed during sysplex communication.</td>
</tr>
<tr>
<td>0F</td>
<td>XCF services failed. RACF will try to restart the RACF datasharing address space.</td>
</tr>
<tr>
<td>10</td>
<td>This abend occurs when a system in datasharing mode is put into failsoft mode because of the occurrence of some other error.</td>
</tr>
<tr>
<td>nn</td>
<td>An internal RACF error has occurred. Contact the IBM support center.</td>
</tr>
<tr>
<td>1C</td>
<td>FOUND: The area to free has a corresponding GETMAIN entry in the tracking table, and the caller specified that it should not have.</td>
</tr>
<tr>
<td>20</td>
<td>NOT FREED: There is a temporary area still allocated at the end of SVC processing.</td>
</tr>
<tr>
<td>A0</td>
<td>A RACF module issued a get-space request. However, register 1 is not equal to zero and does not point to a buffer previously created by the program.</td>
</tr>
<tr>
<td>A4</td>
<td>A RACF module issued a get-space request. However, the subpool in register 0 is not the subpool in which the previously created buffer is allocated.</td>
</tr>
<tr>
<td>A8</td>
<td>A RACF module issued a free-space request. However, register 1 is equal to zero.</td>
</tr>
<tr>
<td>AC</td>
<td>A RACF module issued a free-space request. However, register 1 does not point to the buffer previously created by the program.</td>
</tr>
</tbody>
</table>

Identify and correct the indicated error.

**Problem Determination:** Using IPCS, format the dump taken for this abend. For an explanation of the dump title, see z/OS Security Server RACF Diagnosis Guide.

---

**Explanation:** While RACF was processing a RACROUTE REQUEST=VERIFY, an error occurred in the RACF storage manager.

**System action:** The task ends.

**Programmer response:** Register 15 contains a hexadecimal reason code. (Message ICH409I, if issued, also contains this reason code.)

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>04</td>
<td>BAD LENGTH: The length of the area to get or free is not greater than zero.</td>
</tr>
<tr>
<td>08</td>
<td>BAD ALIGNMENT: The pointer to the area to free is not on a doubleword boundary.</td>
</tr>
<tr>
<td>0C</td>
<td>DUPLICATE FREEMAIN: The area to free has already been freed.</td>
</tr>
<tr>
<td>10</td>
<td>INCORRECT SUBPOOL: The subpool for the area to free is not the subpool in which the area is allocated.</td>
</tr>
<tr>
<td>14</td>
<td>INVALID OVERLAP: Part of the area to free equals part of the area allocated, but the match is not correct for either a full or partial FREEMAIN.</td>
</tr>
<tr>
<td>18</td>
<td>NOT FOUND: The area to free does not have a corresponding GETMAIN entry in the tracking table, and the caller did not specify that it should not have.</td>
</tr>
</tbody>
</table>
FOUND: The area to free has a corresponding GETMAIN entry in the tracking table, and the caller specified that it should not have.

NOT FREED: There is a temporary area still allocated at the end of SVC processing.

A RACF module issued a get-space request. However, register 1 is not equal to zero and does not point to a buffer previously created by the program.

A RACF module issued a get-space request. However, the subpool in register 0 is not the subpool in which the previously created buffer is allocated.

A RACF module issued a free-space request. However, register 1 is equal to zero.

A RACF module issued a free-space request. However, register 1 does not point to the buffer previously created by the program.

Identify and correct the indicated error.

Problem Determination: Using IPCS, format the dump taken for this abend. For an explanation of the dump title, see z/OS Security Server RACF Diagnosis Guide.

Explanation: While RACF was processing a RACROUTE REQUEST=LIST, an error occurred in the RACF storage manager.

System action: The task ends.

Programmer response: Register 15 contains a hexadecimal reason code. (Message ICH409I, if issued, also contains this reason code.)

Code Explanation
04 BAD LENGTH: The length of the area to get or free is not greater than zero.
08 BAD ALIGNMENT: The pointer to the area to free is not on a doubleword boundary.
0C DUPLICATE FREEMAIN: The area to free has already been freed.
10 INCORRECT SUBPOOL: The subpool for the area to free is not the subpool in which the area is allocated.
14 INVALID OVERLAP: Part of the area to free equals part of the area allocated, but the match is not correct for either a full or partial FREEMAIN.
18 NOT FOUND: The area to free does not have a corresponding GETMAIN entry in the tracking table, and the caller did not specify that it should not have.

FOUND: The area to free has a corresponding GETMAIN entry in the tracking table, and the caller specified that it should not have.

NOT FREED: There is a temporary area still allocated at the end of SVC processing.

A RACF module issued a get-space request. However, register 1 is not equal to zero and does not point to a buffer previously created by the program.

A RACF module issued a get-space request. However, the subpool in register 0 is not the subpool in which the previously created buffer is allocated.

A RACF module issued a free-space request. However, register 1 is equal to zero.

A RACF module issued a free-space request. However, register 1 does not point to the buffer previously created by the program.

Identify and correct the indicated error.

Problem Determination: Using IPCS, format the dump taken for this abend. For an explanation of the dump title, see z/OS Security Server RACF Diagnosis Guide.

Explanation: While RACF was processing a RACROUTE REQUEST=DEFINE, an error occurred in the RACF storage manager.

System action: The task ends.

Programmer response: Register 15 contains a hexadecimal reason code. (Message ICH409I, if issued, also contains this reason code.)

Code Explanation
04 BAD LENGTH: The length of the area to get or free is not greater than zero.
08 BAD ALIGNMENT: The pointer to the area to free is not on a doubleword boundary.
0C DUPLICATE FREEMAIN: The area to free has already been freed.
10 INCORRECT SUBPOOL: The subpool for the area to free is not the subpool in which the area is allocated.
14 INVALID OVERLAP: Part of the area to free equals part of the area allocated, but the match is not correct for either a full or partial FREEMAIN.
18 NOT FOUND: The area to free does not have
a corresponding GETMAIN entry in the tracking table, and the caller did not specify that it should not have.

FOUND: The area to free has a corresponding GETMAIN entry in the tracking table, and the caller specified that it should not have.

NOT FREED: There is a temporary area still allocated at the end of SVC processing.

A RACF module issued a get-space request. However, register 1 is not equal to zero and does not point to a buffer previously created by the program.

A RACF module issued a get-space request. However, the subpool in register 0 is not the subpool in which the previously created buffer is allocated.

A RACF module issued a free-space request. However, register 1 is equal to zero.

A RACF module issued a free-space request. However, register 1 does not point to the buffer previously created by the program.

Identify and correct the indicated error.

Problem Determination: Using IPCS, format the dump taken for this abend. For an explanation of the dump title, see z/OS Security Server RACF Diagnosis Guide.

E82

Explanation: SVC 130 (RACROUTE REQUEST=AUTH macro) was invoked; however, SVC 130 is inactive because RACF is not properly installed on the system.

System action: The task stops.

Programmer response: See “Problem Determination.”

Problem Determination: If you have installed RACF on your system, make sure that RACF is properly enabled on your system. For z/OS systems version 1 release 2 or above, the problem may be with your IFAPRDxx member statement in SYS1.PARMLIB used in enabling the product. For details, see the program directory for your system.

E83

Explanation: SVC 131 (RACROUTE REQUEST=VERIFY macro) was invoked; however, SVC 131 is inactive because RACF is not properly installed on the system.

System action: The task stops.

Programmer response: See “Problem Determination.”

Problem Determination: If you have installed RACF on your system, make sure that RACF is properly enabled on your system. For z/OS systems version 1 release 2 or above, the problem may be with your IFAPRDxx member statement in SYS1.PARMLIB used in enabling the product. For details, see the program directory for your system.

E84

Explanation: SVC 132 (RACROUTE REQUEST=LIST macro) was invoked; however, SVC 132 is inactive because RACF is not properly installed on the system.

System action: The task stops.

Programmer response: See “Problem Determination.”

Problem Determination: If you have installed RACF on your system, make sure that RACF is properly enabled on your system. For z/OS systems version 1 release 2 or above, the problem may be with your IFAPRDxx member statement in SYS1.PARMLIB used in enabling the product. For details, see the program directory for your system.

E85

Explanation: SVC 133 (RACROUTE REQUEST=DEFINE macro) was invoked; however, SVC 133 is inactive because RACF is not properly installed on the system.

System action: The task stops.

Programmer response: See “Problem Determination.”

Problem Determination: If you have installed RACF on your system, make sure that RACF is properly enabled on your system. For z/OS systems version 1 release 2 or above, the problem may be with your IFAPRDxx member statement in SYS1.PARMLIB used in enabling the product. For details, see the program directory for your system.
Chapter 12. RACF return codes

This section lists and explains return codes for:
- RACF manager
- RACF utilities

**RACF manager return codes**

This section lists and explains the RACF manager return codes. It contains Programming Interfaces that allow you to write programs to obtain the services of the z/OS Security Server.

The RACF manager returns the codes to the caller (a RACF SVC, a command processor, or a user-written program) in hexadecimal in Register 15.

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (0)</td>
<td>The requested operation was successful.</td>
</tr>
<tr>
<td>4 (4)</td>
<td>A recovery environment could not be established.</td>
</tr>
<tr>
<td>8 (8)</td>
<td>An attempt was made to add an entry (a profile) to the RACF database but an identical entry already exists.</td>
</tr>
</tbody>
</table>

**Note:** Identical entries have the same name, type, and (if specified) volume.

| C (12) | For requests other than NEXT or NEXTC, the specified entry (RACF profile) did not exist. For NEXT or NEXTC requests, no subsequent entries (RACF profiles) 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. The RACF manager uses the EXCP macro to access the RACF database. This error might be caused by a problem with the DASD on which the RACF database is stored. |
| 1C (28) | RACF was not active at the time of the request; or, in an environment with multiple RACF data sets, the RACF data set containing the requested profile is inactive. |
| 19 (25) | The number of actual tests for the ICHEINTY request for the CONNECT type profile is more than 254. |
| 20 (32) | One of the following occurred: |
|     | 1. The request type requires a user work area but the area was not provided (the address in the parameter list was 0). |
|     | 2. For a RENAME, neither NEWNAME nor NEWNAMEX was supplied. |
The input parameter list or the associated ACTION and TEST blocks contain an error. For abend 482, 483, or 485, this RACF manager return code usually indicates that down-level templates are being used for the RACF database. Template conversion is done with IRRMIN00. Do the following:

1. Check the output of IRRMIN00 to be sure higher-level templates were used.
2. Check that the higher level of IRRMIN00 was run.
3. Check that IRRMIN00 was run against the correct RACF database. RACF uses the templates from the first primary RACF database activated.
4. Check that a database with lower level templates was not copied over the database that had IRRMIN00 run against it.

When this code is returned, register 0 contains one of the following reason codes:

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (1)</td>
<td>Entry name (profile name) or NEWNAME is not valid.</td>
</tr>
<tr>
<td>2 (2)</td>
<td>Action(s) specified with DELETE or DELETEA.</td>
</tr>
<tr>
<td>3 (3)</td>
<td>An action specified for an undefined field.</td>
</tr>
<tr>
<td>4 (4)</td>
<td>Test(s) specified with RENAME.</td>
</tr>
<tr>
<td>5 (5)</td>
<td>Reserved.</td>
</tr>
<tr>
<td>6 (6)</td>
<td>Reserved.</td>
</tr>
<tr>
<td>7 (7)</td>
<td>Incorrect entry type (profile type).</td>
</tr>
<tr>
<td>8 (8)</td>
<td>DATAMAP(OLD) was coded on the ICHEINTY macro, and GROUP=YES was coded on the ICHEACTN macro, but the given data length was too long for the repeat group.</td>
</tr>
<tr>
<td>9 (9)</td>
<td>DATAMAP(OLD) was coded on the ICHEINTY macro, and GROUP=YES was coded on the ICHEACTN macro, but the given data length was too short for the repeat group.</td>
</tr>
<tr>
<td>A (10)</td>
<td>Consistency error between multiple input parameter lists. This error occurs if chaining is being used and all input parameter lists are not using the same options or the same values for: TYPE, RBA, CLASS, VOLID, ENTRY, SMC, GENERIC or INDEX.</td>
</tr>
</tbody>
</table>
| B (11) | Input parameter list chaining/request type combination error. This error occurs when the rules for types of input parameter list requests that might be chained are violated. For example, the first input parameter list can only be a NEXT or NEXTC, LOCATE, ALTER or ALTERI, DELETE with SEGMENT or ADD. The following input parameter lists can only be LOCATE (after
LOCATE), NEXT/NEXTC (after NEXT/NEXTC), ALTERI (after ALTERI), ALTER (after ALTER, DELETE or ADD), and DELETE with SEGMENT (after ALTER or DELETE).

C (12) All input parameter lists specify RUN=NO.

D (13) Request type/segmentation combination error. This error occurs if a segment name is specified with ADD, DELETEA, or RENAME.

E (14) Invalid field for GROUP=YES. This error occurs if GROUP=YES was coded but the field is not a repeat group.

F (15) Input parameter list limit exceeded. More than 1000 input parameter lists were chained.

10(16) Segment not allowed. Specified SEGMENT name not allowed for the specified profile TYPE.

11(17) Inconsistency between ACTION data length and repeat group FIELDS, GROUP=YES. This is similar to return code 8, but DATAMAP(NEW) was coded on the ICHEINTY macro.

12 (18) Data length specified on ICHEACTN macro 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 (RDS) format.

15 (21) Invalid NEWNAMX. Current length is greater than 44 and either the primary or the backup database is not in the restructured (RDS) format.

16 (22) Data length specified on the ICHEACTN macro was less than zero and neither FLDATA='DEL' nor FLDATA='COUNT' was specified.

17 (23) The generic entity name exceeds the maximum length after it has been encoded.

18 (24) Limit has been reached for the concurrent source request.

19 (25) Number of tests is greater than 254.

1A (26) Invalid date supplied on an ICHEACTN when DATEFMT=YYYYDDDF is specified.

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) Alias processing not supported for request type.

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.

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; RACF stopped processing.

38 (56) You requested an operation on an entry (profile) in class DATASET that has multiple RACF definitions, but you did not specify a VOLUME to single out a specific entry.

3C (60) For DATASET class 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 IBM-defined entries (such as SYS1 or IBMUSER) from the RACF database.

44 (68) An ALTERI request attempted to increase 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
- The RACF database from a system that is in read-only mode (in a RACF sysplex data sharing environment)

54 (84) Reserved (used internal to RACF).

58 (88) Some field-level access checks failed for data retrieval.

5C (92) All field-level access checks failed for data retrieval.

60 (96) Field-level access checks failed for data update.

64 (100) Reserved for use by the ICHEINTY macro for RELEASE=(xx,CHECK).

68 (104) Invalid data in a RACF profile. Detail code is in the reason code:

<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (1)</td>
<td>Profile too short</td>
</tr>
</tbody>
</table>

6C (108) The RACF manager has been invoked recursively, and an exclusive reserve/enqueue is required. However a shared reserve/enqueue is already held.
The RACF manager received an unexpected return code from a reserve/enqueue. The reserve/enqueue return code is passed back in register 0.

Reserved (used internal to RACF).

Reserved (used internal to RACF).

This is a data sharing mode return code. A coupling facility function had a problem when dealing with the ICB.

Maximum alias index entry size has been reached.

### RACF utility return codes

This topic describes the return codes for the following RACF utilities:

<table>
<thead>
<tr>
<th>RACF utility name</th>
<th>Subtopic name</th>
</tr>
</thead>
<tbody>
<tr>
<td>RACF cross reference utility (IRRUT100)</td>
<td>“IRRUT100 return codes”</td>
</tr>
<tr>
<td>RACF database verification utility (IRRUT200)</td>
<td>“IRRUT200 return codes” on page 410</td>
</tr>
<tr>
<td>RACF database split/merge/extend utility (IRRUT400)</td>
<td>“IRRUT400 return codes” on page 410</td>
</tr>
<tr>
<td>RACF database unload utility (IRRDBU00)</td>
<td>“IRRDBU00 return codes” on page 411</td>
</tr>
<tr>
<td>RACF SMF data unload utility (IRRADU00)</td>
<td>“IRRADU00 return codes” on page 412</td>
</tr>
<tr>
<td>RACF internal reorganization of aliases utility (IRRIRA00)</td>
<td>“IRRIRA00 return codes” on page 412</td>
</tr>
<tr>
<td>RACF remove ID utility (IRRRID00)</td>
<td>“IRR RID00 return codes” on page 413</td>
</tr>
</tbody>
</table>

For utility message explanations, see Chapter 6, “IRR messages for commands, utilities, and other tasks,” on page 185.

### IRRUT100 return codes

For the description and usage details of the IRRUT100 utility, see RACF cross reference utility program (IRRUT100) in z/OS Security Server RACF System Programmer’s Guide.

For message explanations, see “RACF cross-reference utility (IRRUT100) messages” on page 212.

<table>
<thead>
<tr>
<th>Table 2. Return codes for the RACF cross-reference utility (IRRUT100)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hex (decimal)</td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>0  (0)</td>
</tr>
<tr>
<td>4  (4)</td>
</tr>
<tr>
<td>20 (32)</td>
</tr>
</tbody>
</table>
IRRUT200 return codes

For the description and usage details of the IRRUT200 utility, see "RACF database verification utility program (IRRUT200)" in z/OS Security Server RACF System Programmer’s Guide.

For message explanations, see “RACF database verification (IRRUT200) messages” on page 212.

Table 3. Return codes for the database verification utility (IRRUT200)

<table>
<thead>
<tr>
<th>Hex (decimal)</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (0)</td>
<td>Function successful. Report printed.</td>
</tr>
<tr>
<td>4 (4)</td>
<td>A noncritical error was detected. Report printed.</td>
</tr>
<tr>
<td>8 (8)</td>
<td>A critical error was detected. Utility processing might be incomplete. Any</td>
</tr>
<tr>
<td></td>
<td>printed report might be incomplete.</td>
</tr>
<tr>
<td>C (12)</td>
<td>Utility terminated because:</td>
</tr>
<tr>
<td></td>
<td>• A request for storage failed.</td>
</tr>
<tr>
<td></td>
<td>• The inventory control block (ICB) or top-level index block could not be</td>
</tr>
<tr>
<td></td>
<td>read or was not valid.</td>
</tr>
<tr>
<td></td>
<td>• The utility was unable to open a required data set.</td>
</tr>
<tr>
<td></td>
<td>• The database (SYSRACF) and work data set (SYSUT1) device types have</td>
</tr>
<tr>
<td></td>
<td>incompatible track geometries.</td>
</tr>
<tr>
<td></td>
<td>• The same data set was specified for input and output.</td>
</tr>
<tr>
<td></td>
<td>• The output data set is an active RACF data set on this system.</td>
</tr>
<tr>
<td></td>
<td>• DYNALLOC or LOCATE returned an unexpected return code.</td>
</tr>
<tr>
<td></td>
<td>• An error was found in parameter specification.</td>
</tr>
<tr>
<td>20 (32)</td>
<td>RACF is not enabled. Process ends.</td>
</tr>
</tbody>
</table>

IRRUT400 return codes

For the description and usage details of the IRRUT400 utility, see "RACF database split/merge/extend utility program (IRRUT400)" in z/OS Security Server RACF System Programmer’s Guide.

For message explanations, see “RACF database split/merge utility (IRRUT400) messages” on page 227.

Table 4. Return codes for the RACF database split/merge utility (IRRUT400)

<table>
<thead>
<tr>
<th>Hex (decimal)</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (0)</td>
<td>Successful completion without error.</td>
</tr>
<tr>
<td>4 (4)</td>
<td>Duplicate IBM-defined names caused one or more warning conditions.</td>
</tr>
<tr>
<td>8 (8)</td>
<td>One or more error conditions occurred because of one of the following</td>
</tr>
<tr>
<td></td>
<td>reasons:</td>
</tr>
<tr>
<td></td>
<td>• Duplicate non-IBM-defined names.</td>
</tr>
<tr>
<td></td>
<td>• A defective tape volume set.</td>
</tr>
<tr>
<td>C (12)</td>
<td>One or more severe error conditions resulted from an error on an output</td>
</tr>
<tr>
<td></td>
<td>database.</td>
</tr>
</tbody>
</table>
Table 4. Return codes for the RACF database split/merge utility (IRRUT400) (continued)

<table>
<thead>
<tr>
<th>Hex (decimal)</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 (16)</td>
<td>A terminating error condition occurred because of one of the following reasons:</td>
</tr>
<tr>
<td></td>
<td>• A recovery environment could not be established.</td>
</tr>
<tr>
<td></td>
<td>• The SYSPRINT file could not be opened.</td>
</tr>
<tr>
<td></td>
<td>• An error was found in a parameter specification.</td>
</tr>
<tr>
<td></td>
<td>• A range table was requested but could not be loaded.</td>
</tr>
<tr>
<td></td>
<td>• An error was detected in the specified range table.</td>
</tr>
<tr>
<td></td>
<td>• An error occurred on an input database.</td>
</tr>
<tr>
<td></td>
<td>• The same data set was specified for input and output.</td>
</tr>
<tr>
<td></td>
<td>• The output data set is an active RACF data set on this system.</td>
</tr>
</tbody>
</table>

20 (32)       RACF is not enabled. Process ends.

IRRDBU00 return codes

For the description and usage details of the IRRDBU00 utility, see [Using the RACF database unload utility (IRRDBU00)] in [z/OS Security Server RACF Security Administrator’s Guide].

For message explanations, see “RACF database unload utility (IRRDBU00) and RACF SMF data unload utility (IRRADU00) messages” on page 235.

Table 5. Return codes for the RACF database unload utility (IRRDBU00)

<table>
<thead>
<tr>
<th>Hex (decimal)</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (0)</td>
<td>Successful completion without error.</td>
</tr>
<tr>
<td>4 (4)</td>
<td>Error locking or unlocking a data set.</td>
</tr>
<tr>
<td>8 (8)</td>
<td>Failed profile. Conversion is incomplete.</td>
</tr>
<tr>
<td>10 (16)</td>
<td>Terminating error. Conversion incomplete or not started.</td>
</tr>
<tr>
<td></td>
<td>• RACF is not active.</td>
</tr>
<tr>
<td></td>
<td>• Cannot establish recovery.</td>
</tr>
<tr>
<td></td>
<td>• Unexpected or incorrect DD statement found.</td>
</tr>
<tr>
<td></td>
<td>• Incorrect primary or backup dataset specified on INDD1.</td>
</tr>
<tr>
<td></td>
<td>• The utility was unable to open or close a required data set.</td>
</tr>
<tr>
<td></td>
<td>• Specified database could not be unlocked.</td>
</tr>
<tr>
<td></td>
<td>• An error was found in a parameter specification.</td>
</tr>
<tr>
<td></td>
<td>• No parameters were specified.</td>
</tr>
<tr>
<td></td>
<td>• The inventory control block (ICB) or top-level index block could not be read or was not valid.</td>
</tr>
<tr>
<td>20 (32)</td>
<td>RACF is not enabled. Process ends.</td>
</tr>
</tbody>
</table>

IRRADU00 return codes

For the description and usage details of the IRRADU00 utility, see [The RACF SMF data unload utility] in [z/OS Security Server RACF Auditor’s Guide].

Important: The following return codes are returned by the SMF dump utility (programs IFASMFDP and IFASMFDL), not by the IRRADU00 utility, because
IRRADU00 is executed by the SMF dump utility and cannot pass return codes. Therefore, be sure to review the messages produced by IRRADU00 to determine if any problems were encountered.

For message explanations, see “RACF database unload utility (IRRDBU00) and RACF SMF data unload utility (IRRADU00) messages” on page 235.

Table 6. Return codes for the SMF data unload utility (IRRADU00)

<table>
<thead>
<tr>
<th>Hex (decimal)</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (0)</td>
<td>The SMF dump was successful; no errors were encountered. However, IRRADU00 might not unload some records for one or more of the following reasons:</td>
</tr>
<tr>
<td></td>
<td>• Unexpected event code. The numeric value of the event code is unloaded when the event code is unknown. No message is issued.</td>
</tr>
<tr>
<td></td>
<td>• Unexpected relocate section in record.</td>
</tr>
<tr>
<td></td>
<td>• Inability to convert data due to unexpected values.</td>
</tr>
<tr>
<td></td>
<td>• A pre-RACF 1.9 record was encountered.</td>
</tr>
<tr>
<td></td>
<td>• The SMF record type 83 subtype is unknown.</td>
</tr>
<tr>
<td>4 (4)</td>
<td>The SMF dump was successful; one or more errors were encountered but processing continues. IRRADU00 might not unload some records for one or more of the following reasons:</td>
</tr>
<tr>
<td></td>
<td>• Cannot open ADUPRINT.</td>
</tr>
<tr>
<td></td>
<td>• Open failed for specified DDNAME.</td>
</tr>
<tr>
<td></td>
<td>• ABEND during utility processing.</td>
</tr>
<tr>
<td></td>
<td>• Unable to establish recovery environment.</td>
</tr>
<tr>
<td></td>
<td>• RACF is not enabled.</td>
</tr>
<tr>
<td>8 (8)</td>
<td>The SMF dump was not successful; an error terminated processing.</td>
</tr>
</tbody>
</table>

IRRIRA00 return codes

For the description and usage details of the IRRIRA00 utility, see “RACF internal reorganization of aliases utility program (IRRIRA00)” in z/OS Security Server RACF System Programmer’s Guide.

For message explanations, see “Internal reorganization of aliases utility (IRRIRA00) messages” on page 232.

Table 7. Return codes for the internal reorganization of alias utility (IRRIRA00)

<table>
<thead>
<tr>
<th>Hex (decimal)</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (0)</td>
<td>Successful completion.</td>
</tr>
<tr>
<td>4 (4)</td>
<td>Warning message issued.</td>
</tr>
<tr>
<td></td>
<td>• Database already at requested stage.</td>
</tr>
<tr>
<td></td>
<td>• Backup database not converted, currently inactive.</td>
</tr>
<tr>
<td>C (12)</td>
<td>I/O error reading or writing the ICB.</td>
</tr>
</tbody>
</table>
### Table 7. Return codes for the internal reorganization of alias utility (IRRIRA00) (continued)

<table>
<thead>
<tr>
<th>Hex (decimal)</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| 10 (16)       | Terminating error. One of the following occurred:  
  - RACF is not active.  
  - Cannot establish recovery.  
  - Parameter error - unsupported stage value.  
  - Parameter error - unrecognized keyword.  
  - Parameter error - not permitted to convert from current stage to stage value specified.  
  - Failure reading/ updating profile.  
  - Conversion cannot be performed because system is in read-only mode.  
  - Failure writing to CF.  
  - Conversion cannot be performed because templates are downlevel. |
| 20 (32)       | RACF is not enabled. Process ends. |

### IRRRID00 return codes

For the description and usage details of the IRRRID00 utility, see [Using the RACF remove ID (IRR RID00) utility](#) in <I/z/OS Security Server RACF Security Administrator's Guide>.  

For message explanations, see [“RACF remove ID utility (IRR RID00) messages” on page 245](#).

### Table 8. Return codes for the remove ID utility (IRR RID00)

<table>
<thead>
<tr>
<th>Hex (decimal)</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (0)</td>
<td>Function successful. Output generated.</td>
</tr>
<tr>
<td>4 (4)</td>
<td>Function completed. Output is truncated. (See Note.)</td>
</tr>
</tbody>
</table>
| 10 (16)       | Terminating error. Contact IBM service. One of the following occurred:  
  - ESTAE error  
  - DBU record error  
  - OPEN error  
  - SORT error  
  - Internal name index error  
  - Internal message error |
| 20 (32)       | RACF is not enabled. Process ends. |

**Note:** For information about truncated output with the IRRRID00 utility, see [“Using IRR RID00 output: Lengthy commands” in <I/z/OS Security Server RACF Security Administrator’s Guide>](#).
Appendix. Accessibility

Publications for this product are offered in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when using PDF files, you may view the information through the z/OS Internet Library web site or the z/OS Information Center. If you continue to experience problems, send an email to mhvrcfs@us.ibm.com or write to:

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Building 707
2455 South Road
Poughkeepsie, NY 12601-5400
USA

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 such products 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 [TSO/E Primer](http://www.ibm.com/systems/z/os/zos/docs/bksto), [z/OS TSO/E User’s Guide](http://www.ibm.com/systems/z/os/zos/docs/bktso), and [z/OS ISPF User’s Guide Vol I](http://www.ibm.com/systems/z/os/zos/docs/bkisp) 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.

z/OS information

z/OS information is accessible using screen readers with the Library Server versions of z/OS books in the Internet library at:

Notices

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

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
U.S.A

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

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shinotsuruma, Yamato-shi
Kanagawa 242-8502 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:

Site Counsel
IBM Corporation
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.

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

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

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Policy for unsupported hardware

Various z/OS elements, such as DFSMS, HCD, JES2, JES3, and MVS, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Programming interface information

This publication primarily documents intended Programming Interfaces that allow the customer to write programs to obtain services of Security Server.

This publication also documents information that is NOT intended to be used as Programming Interfaces of Security Server.

This information is identified where it occurs, either by an introductory statement to a chapter or section or by the following marking:
Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.
Index

A
abend codes 393
About this document vii
accessibility 415
contact IBM 415
features 415
screen readers 417
ADDGROUP command messages 67
ADDS command messages 86
ADDDUSER command messages 69
administration, RACF classroom courses viii
ALTGROUP command messages 130
ALTUSER command messages 133
assistive technologies 415
Auditx messages 367
C
CACHECLS profile messages messages 313
classroom courses, RACF viii
codes
abend 393
completion 393
descriptor codes 1, 167
RACF manager return codes 405
RACF utility return codes 409
routing codes 2, 168
completion codes 393
CONNECT command messages 72
courses about RACF viii
D
data security monitor (DSMON) messages 154
DB2 external security module for RACF 180
DELDSD command messages 86
DELDGROUP command messages 79
DELUERUSER command messages 76
descriptor codes 1, 167
DISPLAY command messages 273
DSMON (data security monitor) messages 154
dynamic parse messages 186
dynamic started task operator messages 179
F
File allocation messages 350
H
health checker messages 369
How to use this document vii
I
ICH operator messages 1
ICH000 series of messages 3
ICH00000 series of messages 67
ICH01000 series of messages 69
ICH02000 series of messages 72
ICH03000 series of messages 74
ICH04000 series of messages 76
ICH05000 series of messages 79
ICH06000 series of messages 80
ICH08000 series of messages 83
ICH09000 series of messages 86
ICH10000 series of messages 92
ICH11000 series of messages 97
ICH12000 series of messages 102
ICH13000 series of messages 104
ICH14000 series of messages 105
ICH15000 series of messages 119
ICH20000 series of messages 130
ICH21000 series of messages 133
ICH22000 series of messages 138
ICH300 series of messages 4
ICH30000 series of messages 142
ICH31000 series of messages 143
ICH32000 series of messages 146
ICH35000 series of messages 147
ICH400 series of messages 5
ICH500 series of messages 33
ICH51000 series of messages 149
ICH64000 series of messages 152
ICH66000 series of messages 154
ICH700 series of messages 61
ICH70000 series of messages 159
ICH800 series of messages 62
ICH900 series of messages 63
IKJ messages 391
initialization messages 33
intended audience vii
Internal reorganization of aliases utility (IRRIRA00) messages 232
IRR callable services messages 365
IRR operator messages 167
IRR000 series of messages 168
IRR16000 series of messages 186
IRR400 series of messages 171
IRR500 series of messages 177
IRR52000 series of messages 186
IRR61000 series of messages 212
IRR62000 series of messages 212
IRR63000 series of messages 221
IRR65000 series of messages 227
IRR66000 series of messages 232
IRR87000 series of messages 235
IRR86000 series of messages 245
IRR71000 series of messages 247
IRR800 series of messages 177, 178, 179, 180
IRR88000 series of messages 161
IRR9000 series of messages 248
IRRADU00 utility messages 235
return codes 411
IRR80000 series of messages 249
IRRC000 series of messages 257
IRRDO000 series of messages 273
IRRI000 series of messages 276
IRR20000 series of messages 365
IRRD000 utility messages 235
return codes 411
IRRD000 series of messages 365
IRRDP00 command messages 177, 186
IRR00000 series of messages 292
IRRF000 series of messages 295
IRRG000 series of messages 296
IRRH000 series of messages 298
IRRID00 series of messages 300
IRRIR00 utility return codes 412
IRRJ000 series of messages 310
IRRK000 series of messages 311
IRRL000 series of messages 312
IRRL1000 series of messages 313
IRRM000 series of messages 315
IRRMIN00 utility messages 161
IRRN000 series of messages 328
IRRRO00 series of messages 330
IRRP000 series of messages 330
IRRQ000 series of messages 335
IRRRI000 series of messages 336
IRRRI00 utility messages 245
return codes 413
IRR5000 series of messages 343
IRRIO00 series of messages 345
IRRJ000 series of messages 350
IRRUT000 utility messages 212
return codes 409
IRRUT000 utility messages 212
return codes 410
IRRUT400 utility messages 227
IRRUT400 utility (continued)
return codes 410
IRRV000 series of messages 351
IRRW000 series of messages 356
IRWX0000 series of messages 359
IRRY000 series of messages 367

K
keyboard
navigation 415
PF keys 415
shortcut keys 415

L
LISTDSD command
messages 147
LISTGRP command
messages 146
LISTUSER command
messages 142
LookAt message retrieval tool ix

M
mainframe
education xi
manuals
on CD-ROM and DVD viii
miscellaneous messages 149
miscellaneous RACF ICH messages 149

N
navigation
keyboard 415
Notices 417
shortcut keys 415
SIGNOFF command
messages 292
status messages 61
system operator messages 1, 167

P
PASSWORD command
messages 83
PERMIT command
messages 80
PKI
messages 365
publications
on CD-ROM and DVD viii

R
RACDCERT command
messages 276
RACF
messages 185, 385
RACF block update command (BLKUPD) messages 221
RACF commands
messages 65
RACF coupling facility related messages 359
RACF database
initialization messages 161
initialization utility messages 161
split/merge utility (IRRUT400) and (IRRIRA00) messages 227
unload utility messages 235
RACF initialization messages 33
RACF manager
error messages 149
return codes 405
RACF messages
miscellaneous 159
miscellaneous ICH 149
RACF operational modes
messages 359
RACF processing messages 5, 171
RACF remove ID utility messages 245
RACF report writer
messages 152
RACF SMF data unload utility
messages 235
RACF status messages 61
RACF subsystem
messages 248
RACF utilities
return codes 409
RACFRW (RACF report writer)
messages 152
RACLINK command
messages 311, 343, 345
RACMAP command
messages 356
RACPRIV command
messages 356
RACROUTE REQUEST=AUTH VLF
operator messages 177
RACROUTE REQUEST=LIST
messages 312
RACROUTE REQUEST=VERIFY
messages 4
RACROUTE REQUEST=VERIFY NJE
operator messages 178, 180
RACVAR function for REXX execs
messages 247
RALTER command
messages 97
RDEFINE command
messages 92
RDELETE command
messages 102
REMOVE command
messages 74
REQUEST=AUTH operator messages 62
REQUEST=DEFINE operator
messages 63
return codes
RACF manager 405
RACF utilities 409
REXX RACVAR function
messages 247
RLIST command
messages 104
routing codes 2, 168
RRSF (RACF remote sharing facility)
messages 330
RRSF connection local transaction
program
messages 310
RRSF connection receive transaction
program
messages 328
RRSF connection send transaction
program
messages 330
RRSF connection task
messages 335
RRSF enveloping
messages 351
RRSF handshaking
messages 300
RRSF output handling task
messages 336, 345
RRSF parmlib and initialization
messages 296
RRSF send request handling task
messages 295
RVARY command
messages 119

S
SAF initialization operator messages 3
screen readers
accessibility 417
SEARCH command
messages 143
security topics for RACF
classroom courses viii
series of messages 180
SET command
messages 298
SETROPTS command
messages 105
shortcut keys 415
SIGNOFF command
messages 292
status messages 61
system operator messages 1, 167
dynamic started task (IRR800) 179
IBM DB2 external security module for
RACF 180
IRRDP100 command (IRR500) 177
RACF initialization (ICH500) 33
RACF processing (ICH400) 5
RACF processing (IRR400) 171
RACF status (ICH700) 61
REQUEST=AUTH (ICH800) 62
REQUEST=AUTH VLF (IRR800) 177
REQUEST=DEFINE (ICH900) 63
REQUEST=VERIFY (ICH300) 4
REQUEST=VERIFY NJE
(IRR800) 178, 180
SAF initialization (ICH000) 3
UID/GID mapping (IRR800) 179
VERIFY and VERIFYX (IRR000) 168
VLF Cache 180

T
TARGET command
messages 315
U
UID/GID mapping operator
  messages  179
user interface
  ISPF  415
  TSO/E  415
utility return codes  409

V
V1R11 changed information  xvii
V1R11 deleted information  xvii
V1R11 new information  xvii
V1R12 changed information  xvi
V1R12 new information  xvi
V1R13 changed information  xv
V1R13 deleted information  xvi
V1R13 new information  xv
VERIFY and VERIFYX operator
  messages  168
VLF Cache operator messages  180

Z
z/OS Basic Skills information center  xi