z/OS

APARs OA35842 and OA35972: Enhanced RACF support for RACROUTE authorization exits

Preface

This information applies to APARs OA35842 and OA35972 which provide more information to RACROUTE authorization exits about the reason RACF granted an authorization request.

Overview

APARs OA35842 (RACF) and OA35972 (SAF) provide RACF support for post-processing exits to indicate what authority is used to grant an authorization request.

The authority used indicator is provided to the following RACF exits:

ICHRCX02 RACROUTE REQUEST=AUTH post-processing exit.

ICHRFX02 RACROUTE REQUEST=FASTAUTH post-processing exit.

ICHRFX04 RACROUTE REQUEST=FASTAUTH post-processing exit.

ICHRDX02 RACROUTE REQUEST=DEFINE post-processing exit.

Software requirements

Support for APAR OA35842 and APAR OA34259 requires the following software releases:

- z/OS Security Server RACF Version 1 Release 12 (FMID HRF7770)

Updated RACF publications

The chapters of this document supplement the V1R12 level of the following RACF publications:

Chapter	Supplements ...
Chapter 1, "System Programmers Guide updates," on page 1	*z/OS Security Server RACF System Programmer's Guide*
Chapter 2, "Data area updates," on page 3	*z/OS Security Server RACF Data Areas*

Chapter 1. System Programmers Guide updates

This information supplements *z/OS Security Server RACF System Programmers Guide*.

The following RACROUTE REQUEST=FASTAUTH postprocessing exits are updated:

- ICHRFX02. See "ICHRFX02."
- ICHRFX04. See "ICHRFX04" on page 2.

ICHRFX02

Indicators showing what authority was used for granting an authorization request are added to the 16-word work area:

The exit is responsible for saving and restoring certain registers it uses. The RACROUTE REQUEST=FASTAUTH exit parameter list contains a pointer (RFXWA) to a 16-word work area. The exit can use the first 15 words of this area to save and restore registers.

On entry to the exit:

- R1 contains the address of the exit parameter list, which contains a pointer to the 16-word FASTAUTH work area. In the FASTAUTH work area:
  - The 2nd word contains a pointer to the class descriptor table entry used for authorization checking. (The exit must not change the contents of the class descriptor table entry.)
  - The 6th word contains a 2-byte profile type followed by a 2-byte profile length.

    The profile type contains one of the following values.

    0 No information, because profile information was provided to the ICHRFX04 exit.
    1 No profile used.
    2 Discrete profile name in external format.
    3 Generic profile name in internal format.
    6 No profile was found.

    The profile length is the length of the profile name (contained in the 7th word).
  - The 7th word contains a pointer to the profile name used in the authorization check. The type and length of the profile name is contained in the 6th word.
  - The 11th word indicates the authority used to determine authorization. The format of the first two bytes of the 11th word are:

    1... .... Reserved for IBM®'s use.
    .1.. .... Normal authority was used.
    ..1. .... OPERATIONS authority was used.
    ...1 .... Trusted authority was used.
    .... 1... Privileged authority was used.
    .... .000 Reserved for IBM's use.
    0000 0000 Reserved for IBM's use.
  - The 12th word contains the RACF® reason code that REQUEST=FASTAUTH processing has determined up to this point.
  - The 13th word contains the RACF return code that REQUEST=FASTAUTH processing has determined up to this point.

  - The 14th word contains 0 if no profile protecting the resource was found or if the class was RACLISTed by RACROUTE REQUEST=LIST,GLOBAL=YES or by SETROPTS RACLIST. Otherwise it contains a pointer to the profile. The profile is mapped by RACRPE within the ISP data area, documented in *RACF Data Areas*.
  - The 15th word contains 0 or information set by the ICHRFX01 or ICHRFX04 exits if they were invoked and set this word to a value.
- R14 contains the return address.
- R15 contains the address of the exit entry point.

ICHRFX04

The exit's parameter list is updated to include information about the authority used to determine authorization:

This exit is passed the parameter list FXAP, which is located in the primary address space. The parameter list contains the ALET to the data space (GLOBAL=YES or SETROPTS RACLIST) or address space (cross-memory GLOBAL=NO) and the pointer to the profile used for authority checking. The profile is mapped by RACRPE within the ISP data area, documented in *RACF Data Areas*. FXAP also contains the address of the ICHRFX02 parameter list (RFXP or FAST), which is actually the parameter list in the caller's storage and under the caller's key with which FASTAUTH was invoked. The parameter list in turn points to the 16-word FASTAUTH work area. Other information in the FXAP includes the address, type, and length of the profile name used in the authorization check, and the authority (for example, OPERATIONS or trusted) that was used to determine authorization.

Chapter 2. Data area updates

This information supplements *z/OS Security Server RACF Data Areas*.

Updated information about ICHRFXAP (FXAP: RACROUTE REQUEST=FASTAUTH Extended Function Exit Parameter List)

New fields ARFXPVER, ARFXPLEN, ARFXUSED, ARFXNORM, ARFXOPER, ARFXTRST, and ARFXPRIV.

Offsets			Len	Name (Dim)	Description
Dec	**Hex**	**Type**			
20	(14)	UNSIGNED	2	ARFXPVER	Parameter list version:1 - Extension exists if RCVTAUTU bit is on
22	(16)	UNSIGNED	2	ARFXPLEN	Parameter list length
24	(18)	UNSIGNED	2	ARFXUSED	Authorization used to grant access. It is set for post-processing exit only. The 2-byte area has the following format:
		1...		ARFXNORM	Normal authority was used.
		.1..		ARFXOPER	OPERATIONS authority was used.
		..1.		ARFXTRST	Trusted authority was used.
		...1		ARFXPRIV	Privileged authority was used.
		 0000		*	Reserved
		0000 0000		*	Reserved
26	(1A)	UNSIGNED	2	*	Reserved

Constants

Len	Type	Value	Name	Description
1	DECIMAL	1	ARFXV1	Extension exists if RCVTAUTU bit is on.

Updated information about ICHPRCVT (RCVT: RACF communication vector table)

New programming interface, RCVTAUTU.

Offsets			Len	Name (Dim)	Description
Dec	**Hex**	**Type**			
633	(279)	BITSTRING	1	RCVTFLG3	MISCELLANEOUS FLAGS
		1...		RCVTDCDT	1-DYNAMIC CDT IS ACTIVE
		.1..		RCVTPLC	Allow lower case passwords
		..1.		RCVTCFLD	Custom fields are in effect
		...1		RCVTAUTU	Authority used is available to authorization exits

Offsets			Len	Name (Dim)	Description
Dec	Hex	Type			
		 1111		*	Reserved

Cross Reference

Name	Hex Offset	Hex Value	Level
RCVTAUTU	279	10	3

Updated information about ICHRCXP (RCXP: RACROUTE REQUEST=AUTH exit parameter list)

New fields RCXAUSED, RCXANORM, RCXAOPER, RCXAEXIT, and RCXABYPS.

Offsets			Len	Name (Dim)	Description
Dec	Hex	Type			
148	(94)	ADDRESS	4	RCXAUSED	Address of authorization used to grant access. It is set for post-processing exit only. Points to a 2-byte area of the following format:
		1...		RCXANORM	Normal authority was used.
		.1..		RCXAOPER	OPERATIONS authority was used.
		..1.		RCXAEXIT	Installation exit processing was used.
		...1		RCXABYPS	User ID = '*BYPASS*' was used. **Note:** When *BYPASS* is used, the final RACF return code is 4. This might allow access to a resource, depending on the application.
		.... .000		*	Reserved
		0000 0000		*	Reserved

Cross Reference

Name	Hex Offset	Hex Value	Level
RCXABYPS	94	10	2
RCXAEXIT	94	20	2
RCXANORM	94	80	2
RCXAOPER	94	40	2
RCXAUSED	94		2

Updated information about ICHRDXP (RDXP: RACROUTE REQUEST=DEFINE exit parameter list)

New fields RDXAUSED, RDXANORM, RDXASPEC, RDXAOPER, and RDXAEXIT.

Offsets			Len	Name (Dim)	Description
Dec	**Hex**	**Type**			
180	(B4)	ADDRESS	4	RDXAUSED	Address of authorization used to grant access. It is set for post-processing exit only. Points to a 2-byte area of the following format:
		1...		RDXANORM	Normal authority was used.
		.1..		RDXASPEC	SPECIAL authority was used.
		..1.		RDXAOPER	OPERATIONS authority was used.
		...1		RDXAEXIT	Installation exit processing was used.
		 0000		*	Reserved
		0000 0000		*	Reserved

Cross Reference

Name	Hex Offset	Hex Value	Level
RDXAEXIT	B4	10	2
RDXANORM	B4	80	2
RDXAOPER	B4	20	2
RDXASPEC	B4	40	2
RDXAUSED	B4		2

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corporation, 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.

Other company, product, and service names may be trademarks or service marks of others.