SAF Return and Function Codes

- SAF Return Codes
- Return Code Structure
- Internal Function Codes
- Interpreting Trace Messages

SAF Return Codes

The SAF Security Kernel displays an eight-byte code containing various return and reason codes from SAF.

This information is shown in a number of messages denoted "SSSSSSSS".

Return Code Structure

The SAF return code contains the following structure:

Position Within Message Code	Information Content
Byte: 1	SAF return code (R15 after RACROUTE)
Byte: 2	Function code (see section Internal Function Code)
Byte: 3	RACROUTE return code
Byte: 4	RACROUTE reason code
Byte: 5-8	Internal reason code

The SAF trace messages written to DDPRINT, when GWMSGL is not 0, include the first four bytes of this information, printed as eight hexadecimal digits:

Position Within Trace Message	Information Content
Digits 1 and 2	SAF return code (R15 after RACROUTE)
Digits 3 and 4	Function code (see section Internal Function Code)
Digits 5 and 6	RACROUTE return code
Digits 7 and 8	RACROUTE reason code

Refer to the *IBM Security Server RACROUTE Macro Reference* manual for a thorough explanation of all possible return/reason codes. CA-Top Secret and CA-ACF2 can provide different return code values in some circumstances.

Internal Function Codes

SAF Security Kernel internal function codes include:

Function Code (Hex)	Description
00	Authorize Natural Library
04	Authorize Adabas access
08	Authorize SYSMAIN function
0C	Authorize Natural system files
10	Authorize Natural program execution
14	Authorize Broker service
18	Authorize Net-Work access (Net-Work SAF Security) or Adabas cross-level access (Adabas SAF Security) or RPC execution (Natural SAF Security).
1C	Authorize SQL Server access
44 or 6C	AuthenticateUser

Interpreting Trace Messages

The SAF Kernel may optionally write trace messages to DDPRINT (or SAFPRINT). These trace messages have the following format:

```
Time   Jobname  Result     Return Code Type SAF Userid Level Resource Name
13:19:19 DAEFCODE SEF DENIED    08040800 RQ 02 :USERA   : (02) CMD00153.FIL00005
```

Field	Explanation
Time	Time the security check was made.
Jobname	Job that requested the security check. For Adabas and Net-Work SAF Security this is the job that issued the Adabas call being checked.
Result	SEF DENIED: the security system rejected the access attempt. SEF PERMITTED: the security system allowed the access.

Field	Explanation
Return Code	The return code consists of 4 hexadecimal bytes which contain the following information. The numbers in brackets refer to the values in the example trace message above. ● Byte 1 (08) - R15 after RACROUTE ● Byte 2 (04) – internal function code (see table above) ● Byte 3 (08) – RACROUTE return code ● Byte 4 (00) – RACROUTE reason code The return code can be interpreted by checking the RACROUTE manual referred to above for the appropriate RACROUTE function (AUTH for an authorize function; VERIFY for authenticate). For a RACROUTE AUTH, R15 of 8 with return code 8 and reason code 0 means the user is not authorized to use the requested resource. This is a normal security violation. For PERMITTED security checks, the return code contains 00000000 or 00000001. 00000001 indicates that the security check was satisfied from the SAF Kernel’s cache (that is, the same user had previously requested the same resource access and the SAF Kernel had cached the security system’s successful response).
Type	The internal SAF Kernel request type. This may be: ● 01 – authorize Natural library ● 02 – authorize Adabas access ● 03 – authorize SYSMAIN function ● 04 – authorize Natural system files ● 05 – authorize Natural program execution ● 06 – authorize Broker service ● 07- authorize Net-Work (or Adabas cross-level) access ● 08 – authorize SQL server access ● 13 – authenticate user ● 23 – authorize Natural RPC execution
SAF Userid	The SAF User ID for which access was requested.

Field	**Explanation**
Level	The access level requested: ● 02 – read ● 04 – update ● 08 – control ● 80 – alter
Resource Name	The name of the resource for which access was requested. For successful user authentications, resource name contains: ● XXNEWU – user successfully authenticated or ● XX - user already logged on

In the example trace message shown above: at 13:19:19, SAF user USERA in job DAEFCODE attempted to read Adabas file 5 in database 153 but did not have the necessary security access.