⑤ software AG

Adabas SAF Security

Adabas SAF Security Messages and Codes

Version 7.4.2

September 2009

Adabas SAF Security

Table of Contents

1   Adabas SAF Security Messages and Codes

ADASAF Messages

AAF001 Unable to load required modules

Explanation A required module could not be loaded. Operation terminates with an abend U0042.

Action Check that all required modules are available.

AAF002 Unable to allocate required storage

Explanation There is insufficient storage available for ADASAF to operate. Operation terminates with an abend U0042.

Action Increase the amount of storage (above the 16-megabyte line) available to the failing job.

AAF003 dbid Unable to allocate NRS storage

Explanation ADASAF needs approximately 2KB of storage below the 16-megabyte line. If the storage is not available at initialization (or after a `newcopy` operator command), ADASAF issues this message and operation terminates.

Action Ensure that enough storage is available.

AAF004 dbid Module xxxxxxxx not loaded

Explanation The indicated module could not be loaded during initialization or during the `newcopy` operator command. If the module is required (rather than optional), operation terminates.

Action Ensure that the module is available.

AAF005 dbid Invalid parameters detected

Explanation One or more invalid parameters were specified in DDSAF. Operation terminates.

Action Correct the invalid parameters.

AAF006 dbid Allocation of user file cache failed

Explanation ADASAF allocates a user file cache above the 16-megabyte line. If the storage is not available at initialization (or after a `newcopy` operator command), ADASAF issues this message and operation terminates.

Action Ensure that enough storage is available or reduce the `MAXFILES` parameter (this may adversely affect performance).

AAF007 dbid INPUT PARAMETER

Explanation ADASAF echoes the parameters read from DDSAF for information and auditing purposes.

Action None.

AAF008 dbid Invalid parameter: INPUT PARAMETER

Explanation ADASAF detected incorrect input in DDSAF. AAF008 is issued for each invalid parameter found and is followed by message AAF005.

Action Correct the invalid parameter.

AAF009 dbid Allocation of Password/Cipher Code cache failed

Explanation There is insufficient storage available above the 16-megabyte line to allocate the table. Each entry requires 16 bytes and the table has a 32-byte header. Operation terminates.

Action Ensure that enough storage is available.

AAF010 dbid Password/Cipher Code cache too small - increase MAXPC

Explanation ADASAF found more passwords and/or cipher codes in RACF than it could store in its table. Operation terminates.

Action Increase the `MAXPCC` parameter.

AAF011 dbid Error extracting Passwords/Cipher Codes from RACF

Explanation ADASAF could not extract passwords and cipher codes from RACF. Operation terminates.

Action Check that you have specified the correct resource class and entity name format. Activate tracing and check for any errors or warnings. Check the system log for RACF messages.

AAF012 dbid Adabas SAF VX.X.X is active in XXXX mode

Explanation ADASAF has successfully initialized in FAIL or WARN mode, as indicated by XXXX.

Action None.

AAF015 dbid Newcopy of Configuration module failed

Explanation After a `newcopy` operator command, ADASAF was unable to reload SAFCFG. Operation terminates.

Action This error occurs only if there is a shortage of storage or the module SAFCFG was deleted from the load library after initialization. Determine which of these is the case and correct it.

AAF016 dbid Newcopy reinitialization failed

Explanation This message appears after a failure during `newcopy` processing. It should be accompanied by a more detailed error message specifying the nature of the failure.

Action Take the action recommended by the accompanying message.

AAF017 dbid Not APF authorized

Explanation ADASAF must run APF-authorized. Operation terminates.

Action Check that all STEPLIBs are in the APF list and that ADARUN is linked with `AC(1)`.

AAF018 dbid No security details for job JOBNAME

Explanation This message appears when an unsecured Adabas call is received from the indicated job.

Action The most likely cause is an installation error, either of the Adabas Router security extensions or of the Adabas link module.

AAF019 dbid ADASAF initialization error(s) - Nucleus will terminate

Explanation This message appears after an initialization error and is preceded by a more specific error message.

Action Take the action recommended by the accompanying message.

AAF020 dbid Unable to add ADASAF Smart Management PIN

Explanation This message appears during initialization if ADASAF fails to activate its Adabas Error Handling interface.

Action None. ADASAF continues, with its Error Handling interface disabled.

AAF021 dbid NOTOKEN is set - calls from unsecured clients are allowed

Explanation The configuration option `NOTOKEN` has been activated. No security checks will be performed for unsecured mainframe clients. See the configuration parameter `NOTOKEN`.

Action None.

AAF022 dbid Incompatible Configuration module detected

Explanation ADASAF has detected an incompatible Configuration module. The nucleus session terminates.

Action Ensure that the Configuration module is created using the macros supplied with the version of ADASAF you wish to use.

AAF023 dbid Invalid xxxx parameter returned by ADASAFX2

Explanation Your password/cipher code exit has returned incorrect data, as indicated by xxxx:

- type: the returned code type was neither password nor cipher code

- code: no password/cipher code was returned

- file: no file number was returned

The nucleus session terminates.

Action Correct your exit.

AAF024 ADASAF installation error: SAFPMAC not linked REUSable

Explanation ADASAF cannot initialize because the module SAFPMAC has not been linked with the REUS attribute. The nucleus session terminates.

Action Ensure that SAFPMAC is linked REUS, NORENT.

SAF Security Kernel Messages

SAF Security Kernel messages are described in the *SAF Security Kernel* documentation.

Adabas Response Codes

The following Adabas response codes can result from ADASAF processing:

Code	Meaning
200	The command could not satisfy the necessary security checks. This response code may be accompanied by one of the following subcodes:
	■ 0: standard user check failed
	■ 1: no free user file cache entry for workstation user
	■ 2: cross-level security check failed
	■ 3: no security information available for command
	■ 4: timeout during workstation logon
207	Internal ADASAF and ADALNK two-phase response code for remote workstation logon. This code is normally not displayed or presented.
208	ADASAF response code indicating that two-phase logon can continue. If this internal response code is displayed or otherwise presented, the wrong ADALNK version for workstation logon is being used.

Code	Meaning
209	Workstation user's password has expired. This code is normally not returned to the application. Instead the workstation user is prompted to enter a new password.

SAF Return Codes

ADASAF 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 ADASAF 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 below)
Byte: 3	RACROUTE return code
Byte: 4	RACROUTE reason code
Bytes: 5 - 8	Internal reason code

The ADASAF trace messages 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 below)
Digits 5 and 6	RACROUTE return code
Digits 7 and 8	RACROUTE reason code

Refer to the IBM documentation *External Security Interface (RACROUTE) Macro Reference* for MVS and VM 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

ADASAF internal function codes include:

Function Code (Hex)	Description
04	Authorize Adabas access
18	Authorize cross-level access
44 or 6C	Authenticate user

Diagnosis of Violations

If security violation logging is active, the SAF Security Kernel includes additional diagnostic information about the violation in its trace message. This information is described in the *SAF Security Kernel* documentation.

Index