Adabas SAF Security

Adabas SAF Security Installation

Version 7.4.2

September 2009

Adabas SAF Security

This document applies to Adabas SAF Security Version 7.4.2 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Table of Contents

1 Adabas SAF Security Installation

This document describes how to install ADASAF

Prerequisites for Using ADASAF

ADASAF operates with Adabas version 7.1 and above running on OS/390 systems in either single-user or multi-user mode. It is compatible with the following operating systems:

- OS/390 version 2, release 10
- z/OS version 1, releases 1-4
- z/OS.e, releases 3-4. Support for z/OS.e is currently restricted to client programs executing in batch, or under TSO or Com-plete.

For ADASAF to operate correctly, you must also install the Adabas System Coordinator server component (ADAPOP). This is described in more detail in the *Adabas System Coordinator* documentation.

Note: ADASAF does not use the Adabas System Coordinator client or daemon components.

ADASAF requires the following levels for the security system being used with Adabas:

- CA-ACF2 version 5 and above;
- CA-Top Secret version 4.2 and above;
- RACF version 2.1 and above.

Note: When running an Adabas nucleus with ADASAF, Software AG recommends that you use the Adabas router and link routines for the same SM level.

ADASAF also requires the Adabas Limited Library (WAL), which contains the SAF Security Kernel. For information about installing and configuring the SAF Security Kernel, see the *SAF Security Kernel* document included in the Adabas version 7.4.2 documentation.

Installation Datasets

The Software AG System Maintenance Aid procedure copies the ADASAF datasets from the installation tape to disk. For more specific information about the tape contents, refer to the *Report of Tape Creation* that accompanies the ADASAF tape.

Installation Dataset Space Requirements

The datasets are named *AAFvrs*, where *vrs* is the current ADASAF version, revision, and system maintenance level. The following are the DASD space requirements for the ADASAF installation datasets:

Dataset	3380 Disk Space Requirement
AAFvrs.LOAD	15 tracks
AAFvrs.SRCE	10 tracks
AAFvrs.JOBS	2 tracks
AAFvrs.INPL	60 tracks
AAFvrs.ERRN	2 tracks

There may also be a ZAPS dataset containing important last-minute corrections in AMASPZAP format and INPL update datasets containing corrections to the ADASAF online system.

Installation Dataset Members

AAFvrs.JOBS

The dataset *AAFvrs.JOBS* contains the following members:

Name	Equivalent SMA Jobs	Description
SAGI010	I020	Job to authorize ADARUN.
SAGI020	none	Job to specify transaction User IDs for users of CICS version 3 or below.
SAGI030	I010 and I011	Job to link the ADASAF security router (SVC). The job as distributed provides an example for temporary linking; it can be modified for permanent linking.
SAGI050	none	Job to temporarily install the ADASAF router (SVC).
SAGI060	none	Job to assemble the Adabas operator command table ADAEOPTB and link to ADAIOR.
SAGI061	I061	Job to load ADASAF Online Services.

Installation Procedure

Before installing ADASAF, be sure that the prerequisite system configuration is available. Then perform the following steps:

Step 1: Copy the Datasets

Using the Software AG System Maintenance Aid procedure, copy the datasets from the release tape to disk.

To permit ADASAF to issue the required RACROUTE macro requests to the security package, you must ensure that the following requirements are met:

- The Adabas loadlib is APF-authorized (see step 2).
- The Adabas ADARUN module is linked with `AC=1` (see step 3).

Step 2: APF-Authorization

Ensure that the Adabas load library, the ADASAF load library and the Adabas System Coordinator load library are APF-authorized; otherwise, message AAF017 occurs and the Adabas nucleus is terminated.

Step 3: Link ADARUN

Execute the SAGI010 job to link ADARUN with an authorization code of 1.

Step 4: Relink the Adabas SVC

Execute SAGI030 to relink the Adabas SVC with the router security extensions supplied on the Adabas Limited Load library.

Before the ADASAF router can be installed, a set of router security exits must be linked. Currently, the router security extensions protect the following environments:

Environment	Description
Batch and TSO	Adabas calls from ADALNK can be secured by the external security system using ADASAF. The external security User ID is retrieved from the ACEE address in the TCBSENV field or, if TCBSENV is not set, the User ID is retrieved from the ASXBSENV field.
Com-plete or Entire Service Manager	Adabas calls from ADALCO can be secured by the external security system using ADASAF. The external security User ID is retrieved from the ACEE address in the TCBSENV field.
CICS Version 2 and 3	Adabas calls from ADALNC or ADAOLSC can be secured by the external security system using ADASAF. The external security User ID is retrieved from the external security control block pointed to by the SNT or the SNB. RACF and CA-Top Secret users should ensure that external security is set to YES in both the SIT and SNT parameters.
CICS 4.1 or above	The CICS command-level link routine and task related user exit (TRUE) must be used for CICS 4.1 or above. CICS passes the external security identifier as a parameter to the TRUE, which in turn passes the identifier on to the Adabas router. **Note:** The enhanced link routine installation is required in order for ADASAF to operate correctly. In addition, CICS must be configured to use an external security manager. For more information, see the *Adabas Installation* documentation (OS/390, z/OS, OS IV/F4).
IMS Version 2 and 3	Adabas calls from ADALNI can be secured by the external security system using ADASAF. The external security User ID is retrieved from the IOPCB in an IMS environment. External security must enable for the /SIGN transaction.
IMS Version 3 and above	The external security User ID is retrieved from the IOPCB or, for batch regions, from the TCB or ASXB.

To link the security extensions with ADASVC, change the job control for either permanent or temporary installation of the SVC. Examples are provided below and in job SAGI030. For more information, see the *Adabas Installation* documentation.

Permanent Installation

For permanent installation, change the JCL as follows:

```
// EXEC PGM=IEWL
// PARM='XREF,LIST,LET,NCAL,RENT,REUS'
//SYSPRINT  DD SYSOUT=*
//SYSUT1    DD UNIT=SYSDA,SPACE=(CYL,(1,1))
//SYSMOD    DD DSN=SYS1.LPALIB,DISP=SHR     (target loadlib)
//ADALIB    DD DSN=user.loadlib,DISP=SHR     (ADASVC loadlib)
//WALLIB    DD DSN=yourdsn.LOAD,DISP=SHR    (SVCSAF loadlib)
//SYSLIN    DD *
  MODE AMODE(31),RMODE(24)
  CHANGE ADASVC(IGC00nnp)     (see 'Installation Manual')
  INCLUDE ADALIB(ADASVC)
  INCLUDE WALLIB(SVCSAF)
  NAME IGC00nnnp(R)
/*
```

Temporary Installation

For temporary installation, change the JCL as follows:

```
// EXEC PGM=IEWL
// PARM='XREF,LIST,LET,NCAL,RENT,REUS'
//SYSPRINT   DD SYSOUT=*
//SYSUT1     DD UNIT=SYSDA,SPACE=(CYL(1,1))
//SYSLMOD    DD DSN=SYS1.LINKLIB,DISP=SHR   (target loadlib)
//ADALIB     DD DSN=user.loadlib,DISP=SHR   (ADASVC loadlib)
//WALLIB     DD DSN=yourdsn.LOAD,DISP=SHR   (SVCSAF loadlib)
//SYSLIN     DD *
  MODE AMODE(31),RMODE(24)
  INCLUDE ADALIB(ADASVC)
  INCLUDE WALLIB(SVCSAF)
  NAME ADASVC(R)
/*
```

Step 5: Configuration Options

You should review and make any neccessary modifications to the SAFCFG configuration options. For more information, see the section Configuration and also the *SAF Security Kernel* documentation as well as the documentation of any other Software AG SAF Security product you have installed.

The ADASAF source library contains an example member, AAFPARM, which illustrates how to set the SAFCFG configuration options relevant to ADASAF.

Step 6: Assemble and Link the SAF Modules

Assemble and link the site-dependent SAF Security Kernel modules: SAFCFG, SAFPSEC, and SAFPMAC, using the jobs SAFI010, SAFI020 and SAFI021 supplied on the Adabas Limited jobs library. Change the SAFCFG assembly job to reference your configuration module source member. For more information, see the *SAF Security Kernel* documentation.

Step 7: Install the Operator Command Security Exit (optional)

To permit ADASAF to perform security validation for operator commands, modify and execute the supplied sample job SAGI060. This will assemble the command grouping table ADAEOPTB and link it together with ADAIOR and the ADASAF operator command security exit ADAEOPV.

If individual command rather than group checking is to be performed, remove the Include statement for ADAEOPTB. A weak unresolved external reference for ADAEOPTB will be ignored in this case.

Note: ADAEOPV also enables the ADASAF operator commands.

Step 8: Load the Online Services Application SYSAAF (optional)

If you wish to use ADASAF's Online Services application SYSAAF, execute job SAGI061 to load into an appropriate Natural system file.

Note: Software AG strongly recommends that you secure the application SYSAAF using Natural Security. If Natural Security is installed, define the libraries SYSAAF and SYSMX742.

Step 9: Check the STEPLIB Concatenation

The library containing the ADARUN module linked `AC=1` in step 3 must be first in the STEPLIB concatenation for the Adabas start-up procedure.

Also ensure that the ADASAF load library, the target load library used in step 6 (if different), and the Adabas limited load library are APF-authorized and added to your STEPLIB concatenation. Alternatively, copy the modules SAFADA and PINSAF from the ADASAF load library, SAFKRN from the Adabas limited load library, and the SAF Security Kernel modules created in step 6 into an existing APF-authorized step library.

You must also either APF-authorize the Adabas System Coordinator load library and add it to your STEPLIB concatenation or copy the following modules to an authorized step library: ADAPOB, ADAPOP, ADAPOV, CASADA, CORKRN and PINCOR.

If you wish to protect Adabas utilities and single-user mode batch jobs, you must also ensure that the ADASAF, SAF Security Kernel, and Adabas System Coordinator modules listed above are available in the STEPLIB concatenation of those batch jobs. For utilities and single-user mode batch jobs, ADASAF does not have to run APF-authorized.

Step 10: Security Profile and Rule Definitions

Create the necessary security profile and rule (entity) definitions required by the security package. See section Configuration for more information.

Step 11: Check the Job Control

Ensure that the job control contains an appropriate DDPRINT DD statement and, if required, DDSAF and SAFPRINT statements.

Index