Adabas SAF Security

Glossary

Version 8.1.3

June 2008

Adabas SAF Security

This document applies to Adabas SAF Security Version 8.1.3 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

Glossary

Glossary entries exist beginning with the following letters:

A

ACEE Control Block

A control block used by SAF security systems. An ACEE (Accessor Environment Element) control block is built for a user after successfully logging on. It contains:

- User ID, user attributes, and installation data
- point of entry (e.g., terminal) and application
- list of User's Groups (2 lists)

For Adabas, the router must be linked with security exits. These exits extract the User ID from the ACEE for that user.

ADASVC

Adabas Supervisor Call. An internal routine used by Adabas to perform internal communication.

During Adabas SAF installation, the Adabas SVC must be relinked with the router security extensions supplied on the Adabas Limited Load library.

Adabas Basic Services (ABS)

Adabas SAF can be used to incorporate protection of Adabas Basic Services into an SAF security repository. This option can be activated on a nucleus-by-nucleus basis using the ABS parameter.

Adabas System Coordinator

Adabas System Coordinator provides infrastructure technology for the optional Adabas Fastpath, Adabas Vista, Adabas SAF Security and Adabas Transaction Manager features, thereby enabling them to function in the most efficient manner possible.

Adabas SAF Security requires the Adabas System Coordinator. ADASAF needs only the database component (ADAPOP), unless ADASAF's Online Services is to be used in a cluster environment.

For more information, refer to the Adabas System Coordinator documentation.

C

Caching

The results of data access and update checks, both successful and unsuccessful, are cached by ADASAF. There are two levels of caching: A generalized resource cache (see parameter GWSIZE), which contains a given number of user-based entries and holds the profile names for resources that have been successfully checked for this SAF user; and a second cache (see parameter MAXFILES) which is a quick look-up cache and contains an entry for each Adabas user.

CA-ACF2

CA-ACF2 (ACF stands for Access Control Facility), is a set of programs from Computer Associates that enables security on mainframes. CA-ACF2 prevents accidental or deliberate modification, corruption, mutilation, deletion, or viral infection of files. With CA-ACF2, access to a system is denied to unauthorized personnel.

CA-Top Secret

CA-Top Secret from Computer Associates is an external security manager for IBM's OS/390 and z/OS operating systems. Core functions include user authentication, authorization to data sets and a wide variety of resources, including Unix System Services directories and files, and auditing capabilities.

Cipher Code Exits

Assuming that an Adabas command satisfies the appropriate security checks, ADASAF can automatically apply Adabas passwords and cipher codes if the SAF security system is RACF.

The Adabas password and cipher code can be provided by a user exit rather than being stored in RACF.

For more information, see Passwords and Cipher Codes.

Class Descriptor Table (RACF)

If Adabas SAF is being used with the RACF security system, resource classes used must be added to the RACF class descriptor table.

For more information, refer to the IBM RACF documentation.

Cross-Level Security Checking

Cross-level checking allows both the user's and the job's access permissions to be verified. For example, users may be given access to production data but only when they access it from a production TP monitor or batch job.

For more information, see Cross-Level Security Checking.

D

DDSAF

Optional DD statement for overriding ADASAF configuration options in an Adabas nucleus. See DDSAF Parameters.

F

Fail Mode

See also Warn Mode.

When running an ADASAF-protected nucleus in Fail Mode, any security violation causes the Adabas command to be rejected with response 200. ADASAF runs in Fail Mode when the User ID under which the nucleus executes has update access to the nucleus resource profile.

G

Grouped Resource Names

Grouped resource names allow you to reduce security maintenance overheads by defining your own resource names for protection of Adabas data, rather than resource names that are specific to database and file numbers.

For example, if database 153, files 1, 11 and 251 are used for the Accounts Payroll application, instead of defining each file to the security system (as resource name CMD00153.FIL00001 and so on) you can define a single resource, ACCOUNTS.PAYROLL, and configure Adabas SAF Security to use that resource name for files 1, 11 and 251.

M

Multiple Targets

If multiple ADASAF-secured targets are being controlled and these targets reside on different physical machines or nodes, each target node must have the same Logon ID and password assignment per user as every other target node.

MVS Router Table (RACF)

If Adabas SAF is being used with the RACF security system, the MVS router table must be updated.

For more information, refer to the IBM RACF documentation.

O

Online System	An online Natural system (SYSAAF) is available to help monitor and control ADASAF.
Operator Commands	Operator commands are provided for monitoring and controlling ADASAF. See ADASAF Operator Commands.
Operator Command Security	ADASAF may be used to restrict which Adabas operator commands may be issued against an Adabas nucleus. See Adabas Operator Commands.

R

RACF	The IBM Resource Access Control Facility (RACF) is the security system which can be installed on the OS/390 (MVS) operating system. RACF provides access control which determines if a user can gain access to the system, what system resources the user can use once the user has gained access, and how the user may use those resources.
RACROUTE Macro	Macro used to interface with SAF security systems. For more information, refer to the IBM documentation *External Security Interface (RACROUTE) Macro Reference for MVS and VM.*
Resource Class	RACF enables the grouping of similar resource profiles into a resource class. CA-Top Secret and CA-ACF2 provide resource types which give equivalent functionality. For more information, see section Configuration.
Resource Definition Tables	Resource types must be added to the CA-Top Secret resource definition table (RDT). Resource definitions relating to Adabas are kept in resource type ADASEC. For more information, see section Configuration.
Resource Profile	In order to secure Adabas, it is necessary to define resource profiles in the SAF repository. Each SAF-based security system provides the facilities required for maintaining resource profiles. For more information, see section Configuration.

S

SAF Interface	Through the SAF interface, ADASAF requests the proper authority from the external security package.

SAF Security Kernel	The SAF Security Kernel acts as an agent for other Software AG products such as Adabas, Natural, and Entire Net-Work. It allows them to secure resources via a SAF-compliant security system, thus enhancing the scope of the security system.
System Authorization Facility (SAF)	Adabas SAF Security (ADASAF) provides protection of Adabas resources using standard security packages based on the System Authorization Facility (SAF). These security packages include IBM's RACF, and Computer Associates' Top Secret and ACF2.

U

User Cached Files	Storage used for caching user information related to the security system. See also Caching.

W

WAL	Abbreviated notation used for the Adabas Limited Load Library. For more information, refer to the *Adabas Installation* documentation.
Warn Mode	See also Fail Mode. When running an ADASAF-protected nucleus in Warn Mode, ADASAF performs all security checks and traces violations (if tracing is active). However, security violations do not cause a response 200 to be returned. Instead the command is allowed to proceed. ADASAF runs in Warn Mode when the User ID under which the nucleus executes does not have update access to the nucleus resource profile, but does have read access.