An Introduction to Adabas SAF Security

This document provides an introduction to Adabas SAF Security (ADASAF).

- Benefits and Features
- Adabas Resource Protection
- Operation

Benefits and Features

The System Authorization Facility (SAF) is used by z/OS and compatible sites to provide rigorous control of the resources available to a user or group of users. Security packages such as RACF, CA-ACF2, and CA-Top Secret allow the system administrator:

- to maintain user identification credentials such as User ID and password; and
- to establish profiles determining the datasets, storage volumes, transactions, and reports available to a user.

The resulting security repository and the infrastructure to administer it represent a significant investment. At the same time, the volume of critical information held by a business is constantly growing, as is the number of users referencing the data. The challenge of controlling these ever-increasing accesses requires a solution that is flexible, easy to implement and, above all, one that safeguards the company’s investment.

Adabas SAF Security (ADASAF) enhances the scope of SAF-based security packages by integrating Adabas resources into the central security repository. ADASAF enables

- a single control and audit system for all resources;
- industry-standard protection of Adabas data;
- maximized return on investment in the security repository.

Adabas Resource Protection

ADASAF can be used to protect the following Adabas resources:

Resource	Protection
Database Nucleus	Only authorized users are allowed to start an Adabas nucleus.
Adabas Utilities	Only authorized users are allowed to execute utilities, and then only the appropriate ones. Authorization can be restricted by utility as well as Database ID. For example, a user or group of users might be permitted to run ADAREP but not ADASAV against a particular database.
Database Files	Users or groups of users can be permitted (or denied) access to the basic resource of database files.
Database Commands	Access (`READ/FIND`) and update (`STORE/UPDATE/DELETE`) privileges can be granted to specific users or groups of users. To optimize performance, ADASAF disregards commands such as `RC` that are not file-specific.
Production Environment Data	Distinction can be made between a user operating in a production system and the same user operating in a test environment. This is known as cross-level checking and could be used, for example, to prevent damage by an application program inadvertently cataloged against the wrong Database ID.
Transaction Data	ADASAF can optionally validate requests to store or retrieve `ET` data.
Adabas Operator Commands	Restrictions can be placed on Adabas operator commands that can be issued from the MVS console.
File Passwords and Cipher Codes	Passwords and codes can be held in the security repository or supplied by a user exit and dynamically applied by ADASAF. This eliminates the need for the application to manage security data and removes the requirement to transmit sensitive information from the client to the database.
Adabas Basic Services	Adabas Basic Services can be protected with ADASAF by selecting the level of protection required (main functions only or main functions and subfunctions) and defining the appropriate resource profiles and granting the necessary users access to those profiles.
Stored Procedures	Only authorized users are allowed to invoke stored procedures.

You can also protect the online administration components for Adabas SAF Security (SYSAAF), Adabas Fastpath (SYSAFP), Adabas Transaction Manager (SYSATM), Adabas Vista (SYSAVI) and Adabas System Coordinator (SYSCOR) by running the security service in your System Coordinator daemon, and making the appropriate security definitions of course.

Operation

ADASAF operation can be customized on a nucleus-by-nucleus basis, allowing great flexibility in its implementation. To assist in effective usage, an Online Services application, SYSAAF, can be used to monitor and administer ADASAF. ADASAF also provides an error handling facility that is activated automatically at initialization, aiding problem diagnosis.