

z/OS SECURITY MANAGEMENT SUITE. RCF ADMINISTRATION



Administration tasks must be done quickly and with minimum effort. The RACF Administration RCF provides improved handling of your RACF data, in order to support RACF security administrators, auditors and even end users in their daily tasks. With the RACF Administration it becomes easier to ensure the protection of your vital system resources and to define what users are allowed to do on the system.

Benefits

- Easy-to-use RACF administration for all users - even end users - improves security and reduces costs
- Transparent and clear security overview
- Increases the productivity of RACF administrators
- Automatic generation of RACF commands
- Verification of the change authorization
- Full function security and data integrity
- Lots of display capabilities for individual views
- Multi-purpose usage for security administrators, operators and auditors
- Interface to the RACF Auditing RCA
- Helps you providing your installation with the most comprehensive practical protection
- List administration function

RCF provides RACF administration

functions with a user-friendly RACF interface, from which the respective RACF commands are then automatically generated. This RACF front end makes it easy to handle RACF definitions and to provide a comprehensive overview of the information contained in the RACF system. The RCF user and group administrator functions will help you to administer RACF group and user profiles within the administrator's scope of group.

Efficient profile management functions are provided for tasks such as copying, deleting, updating and renaming profiles. New RACF profiles can be created by cloning existing ones and modifying them.

Standard Administration Tasks for users and groups

- Reset user passwords
- Resume userids
- Change user and group profile definitions
- Add and change RACF user segments
- Revoke users
- Connect users to groups
- Remove users from groups
- User authorization administration
- Change user names

In addition to the normal RACF processing expiration and/or permission dates can be specified for data set and general resource profiles.

All defined permission and expiration dates are shown in the corresponding profile panels.

Benefits using permission and expiration dates

- Profiles are automatically deleted at the specified expiration date
- Permits are added to the access list of the profile at the specified permission date
- Permits are removed automatically from the access list of the profile on the date specified as expiration date

Special RACF profiles in the class FACILITY let you control the availability of some RACF administration and audit functions.

The RACF Administration program provides all users with a list administrator function. This function lets a user display all administrators which are able to alter the user's RACF base segment.

A set of TSO commands is offered to list MVS Open Edition information from the OMVS segment for groups and users.

Related Services

- z/OS Security Management consulting