

RACF Administration & Auditing

Course Summary

Description

This four-day, hands-on class is the definitive RACF course for technicians and administrators. The course, designed and written by RACF specialists, is regularly revised and updated to reflect new functionality and features in the RACF and z/OS environments.

The course introduces and explains the concepts, terminology, commands, and procedures involved in administering and auditing RACF. All significant aspects of day-to-day RACF administration and auditing are fully covered. To ensure full understanding, a number of realistic practical exercises are performed throughout this course.

Objectives

At the end of this course, students will be able to:

- Explain the need for security in business information systems
- Describe how racf meets business information systems security needs
- Design a group structure to meet their installation's requirements
- Explain & use racf commands
- Describe the effect of the various group profile related parameters
- Explain the management and use of the various non-racf segments in user profiles
- Connect users to groups and manage the assigned group authorities
- Use the dataset related commands to manage both discrete and generic profiles
- Manage general resources
- Use and explain the operation of the basic setropts management commands
- Use and interpret the output of the data security monitor
- Use the database unload utility, cross reference utility, remove id utility, database verification utility, database split/merge/extend utility, and the database block update utility
- Run and interpret auditing reports.

Topics

- | | |
|-------------------------|------------------------------|
| • Introduction to RACF | • Defining Users |
| • The RACF Manuals | • Connecting Users to Groups |
| • Planning for Security | • Dataset Profiles |
| • Group Structure | • General Resource Profiles |
| • The RACF Commands | • Auditing RACF |
| • Defining RACF Groups | • RACF Utility Programs |

Audience

RACF Administrators and Auditors, Systems Programmers and any other technicians requiring a knowledge of RACF administration principles and practices.

Prerequisites

Attendees should have a clear understanding of z/OS at a conceptual and practical level. A working knowledge of TSO/ISPF and JCL is also required.

Duration

Four days

RACF Administration & Auditing

Course Outline

I. Introduction to RACF

- A. What is RACF?
- B. Why do we need security?
- C. Security in the 'old days'
- D. Security these days
- E. What security do we need?
- F. Where are the dangers?
- G. How can RACF help?
- H. RACF profiles
- I. How RACF operates
- J. The RACF database
- K. Multiple data set database
- L. Resource classes.

II. The RACF Manuals

- A. The manual library
- B. RACF Security Administrators' Guide
- C. RACF features
- D. z/OS features
- E. Other products
- F. Related non-RACF manuals
- G. RACF command language reference
- H. BookManager and Adobe pdf.

III. Planning for Security

- A. The Security Policy
- B. Resource ownership
- C. How to protect resources?
- D. Grouping resources and users
- E. Document the plan.

IV. Group Structure

- A. What are Groups?
- B. Why have Groups?
- C. Users and Groups
- D. The initial group structure
- E. The Group Hierarchy
- F. System Special and Group Special
- G. Group Profile ownership
- H. Group connections.

V. The RACF Commands

- A. Entering RACF commands
- B. RACF commands and the manuals
- C. Entering RACF commands in batch
- D. Entering commands via a CLIST
- E. Online Help.

VI. Defining RACF Groups

- A. Group profile commands
- B. Basic ADDGROUP
- C. Specifying the SUPerior GROUP & OWNER
- D. Other ADDGROUP parameters
- E. Non-RACF segments - DFP, z/OS and zVM
- F. Full ADDGROUP syntax
- G. Full ALTGROUP syntax
- H. Full LISTGRP syntax
- I. LISTGRP output
- J. Full DELGROUP syntax
- K. Group command authority
- L. SEARCH command.

VII. Defining Users

- A. User profile commands
- B. Basic ADDUSER
- C. Specifying the default group
- D. Group authority
- E. Class authority
- F. RACF authorities
- G. RACF attributes
- H. Security levels and security categories
- I. Security level checking
- J. Security category checking
- K. Security labels
- L. Other ADDUSER parameters
- M. Non-RACF segments
- N. Full ADDUSER syntax
- O. Basic ALTUSER
- P. ALTUSER-only parameters
- Q. Full LISTUSER syntax
- R. LISTUSER output
- S. Full DELUSER syntax
- T. User command authority
- U. Basic PASSWORD
- V. Changing other users' passwords
- W. Full syntax of PASSWORD
- X. Password command authority.

VIII. Connecting Users to Groups

- A. Connect and Remove Commands
- B. Basic CONNECT
- C. Full CONNECT Syntax
- D. Basic REMOVE
- E. Full REMOVE Syntax
- F. Connect/Remove command authority.

RACF Administration & Auditing

Course Outline (cont'd)

IX. Dataset Profiles

- A. Dataset profile commands
- B. Basic ADDSD
- C. Discrete dataset profiles
- D. Discrete profile parameters
- E. Generic dataset profiles
- F. Generic wildcard characters - %
- G. Generic wildcard characters - *
- H. Generic wildcard characters - **
- I. Specifying dataset attributes
- J. Access levels
- K. Auditing access attempts
- L. Profile copying
- M. Security level & category checking
- N. Other profile attributes
- O. Full ADDSD syntax
- P. Basic ALTDSD
- Q. ALTDSD-only parameters
- R. Full ALTDSD syntax
- S. Basic LISTDSD
- T. Listing many dataset profiles
- U. Listing generic or discrete profiles
- V. Specifying what to list
- W. Full LISTDSD syntax
- X. LISTDSD output
- Y. Full DELDSD syntax
- Z. Dataset command authority
- AA. Basic PERMIT
- BB. Conditional access lists
- CC. Permitting many users access;
Removing users and groups
- DD. Deleting access lists
- EE. Full PERMIT syntax
- FF. PERMIT command authority
- GG. SETROPTS REFRESH
GENERIC(data set)
- HH. SEARCH command basics
- II. SEARCH control parameters
- JJ. The FILTER & MASK parameters.

X. General Resource Profiles

- A. General resource profile commands
- B. Basic RDEFINE
- C. Common RDEFINE parameters
- D. Adding additional profile information
- E. When the class is CONSOLE
- F. When the class is OPERCMDS
- G. When the class is CDT

- H. When the class is SURROGAT
- I. The Started Task Table; Using
ICHRIN03
- J. Using the STARTED class
- K. When the class is TAPEVOL
- L. Full RDEFINE syntax
- M. Resource grouping classes
- N. Protecting CICS transactions
- O. Protecting load modules
- P. Protecting SDSF
- Q. Basic RALTER
- R. RALTER-only parameters
- S. Full RALTER syntax
- T. Basic RLIST
- U. Common RLIST parameters
- V. Listing Non-RACF segments
- W. Special RLIST features
- X. Full RLIST syntax
- Y. RLIST output
- Z. Full RDELETE syntax
- AA. Remember PERMIT?
- BB. General resource command authority
- CC. The Global Access Checking table
- DD. In-storage profiles
- EE. In-storage profile parameters.

XI. Auditing RACF

- A. Auditing RACF
- B. Auditor parameters
- C. RACF Report Writer
- D. Basic RACFRW commands
- E. Full RACFRW syntax
- F. Full SELECT syntax
- G. Basic EVENT command
- H. Full EVENT syntax
- I. Full LIST syntax
- J. RACFRW output example
- K. Full SUMMARY syntax
- L. RACF SMF data Unload utility
- M. SMF Unload utility JCL
- N. Using the unloaded RACF SMF data
- O. Processing the RACF SMF data with
Db2
- P. Other reporting tools
- Q. The Data Security Monitor
- R. The System & Group Tree Reports
- S. Program Properties & Auth Caller Table
Reports

RACF Administration & Auditing

Course Summary (cont'd)

- T. Class Descriptor Table & RACF Exits Report
- U. Global Access Table Report
- V. Started Procedures Table Report
- W. Selected User Attribute Reports
- X. Selected Data Sets Report.

XII. RACF Utility Programs

- A. The database unload utility
- B. The database cross-reference utility
- C. The database cross-reference utility output
- D. The RACF remove ID utility
- E. The database verification utility
- F. The database split/merge/extend utility
- G. The database block-update utility command.