Course Outline

ProTech Professional Technical Services, Inc.

protechtraining.com

RACF: Advanced Administration

Course Summary

Description

This three-day, hands-on course is the natural follow-on to RSM's definitive RACF Administration & Auditing course for all RACF Administrators. It enables attendees to build on the knowledge and skills they have gained previously with further advanced skills and techniques. In this course experienced RACF Administrators will learn how to handle the more technically challenging aspects of using RACF in today's z/OS environments. The course is packed with challenging, practical, hands-on exercises that will reinforce what attendees learn during the classroom sessions.

Objectives

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

- Describe and explain in detail the RACF architecture, its components, and facilities.
- Understand and use the SETROPTS and RVARY command to manipulate the RACF options and database.
- Use Advanced General Resources classes.
- Define users to use TSO.
- Define the parameters needed to set up security for JES2 and SDSF.
- Describe the facilities provided by RRSF.
- Describe the B1 Security parameters including Security labels, levels, and categories.
- List what facilities RACF provides for Digital Certificates.

Topics

- What is RACF?
- Defining TSO Users
- Advanced General Resources
- RACF & JES2/SDSF
- RACF & Digital Certificates
- RACF Remote Sharing Facility
- Security Labels
- SETROPTS and RVARY

Audience

Those who can benefit from this RACF: Advanced Administration course include:

- All Security Administrators and Systems Programmers

Prerequisites

- A clear understanding of RACF at both the conceptual and practical level.
- RACF Administration & Auditing

Duration

Three days

RACF: Advanced Administration

Course Outline

I. What is RACF?

A. Why do we need security?
B. What does security provide?
C. How does RACF work?
D. RACF profiles
E. RACF classes
F. Controlling access
G. RACF commands

II. Defining TSO Users

A. TSO & RACF
B. The TSO segment of a user profile
C. TSO General Resource classes
D. TSO/E logon screen
E. TSO administration
F. When the class is CONSOLE
G. When the class is OPERCMDS

III. Advanced General Resources

A. Class Descriptor Table (CDT)
B. Dynamic CDT
C. Defining a Dynamic CDT
D. Rules
E. POSIT values
F. New segment CDTINFO
G. CDTINFO option
H. Managing Dynamic CDTs
I. Migration Utility (CDT2DYN)
J. ICHRFR01
K. Normal rules apply
L. When the class is CDT
M. The FACILITY class
N. The Help Desk function
O. Facility class profiles
P. Password reset granularity
Q. ALTUSER changes
R. LISTUSER changes
S. Group/User structure – example
T. Group/User structure – z/OS 1.10
U. Group Tree structure
V. Granular authorities
W. ALTUSER: Allow by Owner
X. ALTUSER: Allow by Tree
Y. Password reset authority scoped by Owner/Tree
Z. LISTUSER authority scoped by Owner/Tree
AA. RACF variables
BB. Using the RACFVARS class
CC. Using RACF variables
DD. Field level access checking
EE. Using the FIELD class
FF. FIELD class examples
GG. Delegating TSO Administration
HH. Security administration for z/OS UNIX
II. Custom Fields
JJ. Customer Fields – preview of results
KK. What is in a Custom Field?
LL. RACF command changes
MM. Defining a Custom Field
NN. Activating a Custom Field
OO. Putting data into a Custom Field
PP. Authorization to define a Custom Field
QQ. Authorization for CSDATA
RR. RACF panel enhancements
SS. Operations attribute
TT. DASD volume operations
UU. Allowing access to DASD volumes
VV. DASDVOL profiles: DF/SMSdss
WW. DASDVOL profiles: ICKDSF
XX. DASDVOL profile authority summary
YY. DASDVOL example
ZZ. Tape security
AAA. Tape volume protection
BBB. Tape dataset protection
CCC. Tape dataset and TAPEVOL protection
DDD. Bypass Label Processing
EEE. Restricting use of BLP

IV. RACF & JES2/SDSF

A. RACF & JES2
B. JES resources protected by RACF
C. Batch user identification
D. Userid propagation
E. Surrogate Job Control
F. JES Early verification; Started Task identification
G. SETROPTS options for JES
H. Network Job Entry (NJE)
I. Remote Job Entry (RJE)
J. z/OS security environment
K. Resource classes for JES security
L. Securing jobs with RACF
M. Job input processing
N. Job submission control
O. Job validation
P. JES job input sources
Q. JESINPUT - controlling Port-Of-Entry device names
R. Job name control
S. TSO SUBMIT/CANCEL commands
T. SURROGAT class
U. Surrogate job submission
V. Job input processing: PROPCNTL & SECLABEL
W. Nodes class
X. NJE security
Y. Controlling transmission to other nodes
Z. Controlling receipt of jobs & sysout
AA. Propagation through NJE

Course Outline (con't)

BB. Translation between nodes
CC. RJE/RJP signon & logon security
DD. Controlling output destinations
EE. Security overlays with PSF
FF. Spool protection
GG. JES dataset name format
HH. JESPOOL class profiles
II. Controlling messages
JJ. Controlling data transmission
KK. SDSF
LL. SDSF authorized commands
MM.SDSF line & implicit commands

V.RACF & Digital Certificates

A. Cryptography in Internet applications
B. Public key cryptography overview
C. What is a digital certificate?
D. Public key & certificate
E. Uses for certificates in applications
F. Secure Sockets Layer (SSL)
G. Digital certificates and RACF
H. How RACF uses digital certificates
I. RACF classes & commands
J. RACDCERT
K. RACF certificate generation
L. RACDCERT command
M. Examples of the RACDCERT command
N. Creating a certificate
O. Gencert examples
P. Key rings
Q. RACDCERT ring functions
R. Certification installation
S. RACDCERT ADD examples
T. Certification installation
U. Certificate management
V. Exploiters of certificates
W. Exporting a certificate
X. Certificates are packaged in formats
Y. Steps for migrating a certificate and its ICSF private key in the PKDS
Z. KEYXFER Utility
AA. Renew a certificate
BB. Examples of REKEY and ROLLOVER
CC. Certificate mapping
DD. Miscellaneous issues
EE. RACF Key Ring protection classes
FF. Global FACILITY class profiles
GG. Sharing a private key
HH. RDATALIB Class
II. RDATALIB – examples
JJ. RACDCERT granular administration
KK. RACDCERT granular control
LL. Listing, removing & deleting
MM.Password enveloping
NN. How does password enveloping work?
OO. Password enveloping - exceptions

VI. RACF Remote Sharing Facility

A. The RACF Remote Sharing Facility
B. RACF command direction
C. RACF password synchronization
D. Managed user associations
E. Controlling RACLINK use
F. Controlling password synchronization
G. Controlling the AT keyword
H. Automatic RACF command direction
I. Controlling automatic RACF command direction
J. Combined RACF command direction
K. Use of ONLYAT keyword
L. Automatic password synchronization
M. Controlling automatic password synchronization
N. Password synchronization by command
O. Combined RACF command direction
P. Defining RRSF nodes
Q. The RACF subsystem & parameter library
R. When the class is APPCLU.

VII. Security Labels

A. What is multilevel security?
B. Security classification
C. Security labels - B1 support
D. Resource authorization checking
E. Security levels
F. Security categories
G. Security labels
H. Defining security levels & categories
I. Defining security labels
J. Assigning security labels
K. SECLABEL class active
L. SECLABEL class active & MLS
M. Dominance & equivalence
N. MAC scenario - user logon
O. MAC scenario - access attempt
P. Security classification options
Q. External access to internal systems

VIII. SETROTS and RVARY

A. The RVARY command
B. RVARY passwords
C. Basic SETROPTS
D. Dataset related parameters
E. General parameters
F. In-storage profile parameters
G. B1 security parameters
H. JES parameters
I. Userid & password parameters
J. Auditor parameters
K. SETROPTS LIST examples
L. SETROPTS command authority