ProTech "Charting the Course ...
protechtraining.com
... to Your Success!"

IBM Security zSecure RACF and SMF Auditing (TK242G)

Course Summary

Description

This course describes the audit concerns reported by IBM® Security zSecure™ Audit. The course explains how to audit the content of your Resource Access Control Facility (RACF®) database and z/OS® system. You can measure your current security settings against the security requirements of a selected policy level. In addition, you learn about an Access Monitor data set that contains statistics about all RACF decisions taken. This information is helpful for finding profiles, permissions, or connections that are not used and can, therefore, be removed from the RACF database. Furthermore, you learn how to review the current general Service Management Framework (SMF) and RACF audit settings. This course explains how to use and interpret the pre-defined SMF audit reports, and how to create your own customized SMF reports. Finally, the concepts of the Library status and change analysis functions are explained and demonstrated.

Objectives

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

- Describe the flow of a security call from Resource Managers to RACF
- Perform user ID and password audit analysis
- Use the audit functions to report on sensitive user IDs and z/OS resources
- Create audit reports on key RACF and z/OS system tables
- Create audit reports for the CICS, IMS, and DB2 subsystems
- Review the system-wide Audit settings
- Select and process predefined SMF reports
- Define custom SMF reports
- Utilize the Access Monitor reports
- Clean up the RACF database
- Audit changes to system-sensitive libraries

Topics

- Introduction to RACF Auditing
- Audit Users and Passwords
- Audit Resources
- Audit Subsystems
- Generate SMF Audit Reports
- Access Monitor and RACF Offline
- Library Analysis

Audience

This intermediate-level training is targeted for RACF security administrators and auditors who are responsible for administering and generating reports, and auditing RACF and z/OS security. RACF and z/OS compliance officers also benefit from attending this training.

Prerequisites

Before taking this course, you should have a basic knowledge of, and experience with, the z/OS platform, RACF, and zSecure. You should also have the ability to log on to TSO and use ISPF panels

Basic RACF and IBM Security zSecure education is assumed and can be obtained in the following classes:

- Basics of z/OS RACF Administration
- Effective RACF Administration
- IBM Security zSecure Admin Basic Administration and Reporting

Duration

Two days

IBM Security zSecure RACF and SMF Auditing (TK242G)

Course Outline

I. Introduction to RACF Auditing
- A. List the RACF resources that need to be audited
- B. Generate and interpret an audit concerns report
- C. Identify all the profiles owned by a particular user
- D. Identify the users authorized to maintain RACF application segments

II. Audit Users and Passwords
- A. Generate and interpret user reports
- B. Identify last logon and password aging
- C. Identify users with system-wide authorities
- D. Identify users with group specific authorities
- E. Generate a report of trusted users

III. Audit Resources
- A. Identify sensitive profiles and the users who can modify them
- B. Identify users who can create profiles of various types
- C. Audit started tasks and programs

IV. Audit Subsystems
- A. Generate audit reports about CICS regions, transactions, and programs
- B. Generate audit reports about IMS regions, transactions, and program specification blocks
- C. Generate audit report about DB2 region

V. Generate SMF Audit Reports
- A. Explain the concepts of SMF auditing
- B. Report which events are logged in SMF
- C. Select events logged in SMF using ISPF interface
- D. Report SMF events with predefined reports
- E. Create customized SMF reports

VI. Access Monitor and RACF Offline
- A. Explain the Access Monitor functions and reports
- B. Generate access summary overview reports
- C. Compare historic access events against current RACF database definitions
- D. Analyze permit, connect, profile, member, and global access entry usage
- E. Remove unused profiles and authorizations
- F.Use the RACF Offline component combined with Access Monitor

VII. Library Analysis
- A. Track changes that occur in z/OS system sensitive libraries