IBM Security zSecure RACF and SMF Auditing Information

Length:	2.0 Days
__Ref:	TK243G-X
Delivery method:	Classroom
Price:	EUR

Overview

This course describes audit concerns that IBM® Security zSecure™ Audit reports. The course explains auditing your RACF® database and z/OS subsystems such as CICS, IMS, and DB2. You can measure your security and z/OS system settings against the security requirements of a selected policy level. Also, you learn about an Access Monitor data set containing historic RACF access decisions statistics. This information is used to find profiles, permissions, or connections that are unused and can be removed from the RACF database. Furthermore, you learn reviewing the general SMF and RACF audit settings. This course explains how to use and interpret predefined SMF reports, and how to create customized SMF reports. Finally, the Library and sequential data set status and change analysis functions are explained.

Public

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

Prerequisits

Before taking this course, make sure that you have the following skills:

- Basic knowledge of, and experience with, the z/OS platform, RACF, and zSecure
- The ability to log on to TSO and use ISPF panels

If applicable, you can achieve these skills by attending one or more of the following courses:

- IBM Security zSecure Admin Basic Administration and Reporting TK263
- Basics of z/OS RACF Administration ES19G
- Effective RACF Administration BE87G

Objective

- Describe and explain the flow of a security call from z/OS and resource Managers to RACF

- Describe and explain the flow of a security call from z/OS and resource Managers to RACF
- Perform user ID and password audit analysis
- Audit sensitive user IDs and z/OS resources and create audit reports about who can define RACF profiles
- Create audit reports for the CICS, IMS, and DB2 subsystems
- Review the system-wide Audit settings, select and process predefined SMF reports, and define custom SMF reports
- Utilize the Access Monitor reports to clean up the RACF database
- Audit changes to system-sensitive libraries and sequential data sets

Topics

Unit 1: Introduction to RACF auditing
Unit 2: Auditing user IDs and passwords
Unit 3: Auditing sensitive resources
Unit 4: Auditing subsystems
Unit 5: Auditing SMF
Unit 6: Using Access Monitor and RACF-Offline
Unit 7: Analyzing libraries and sequential data sets