IBM Security zSecure Course Offerings

Standard zSecure education courses that IBM offers to customers

May 2024

Tom Zeehandelaar

Table of Contents

IBM Security zSecure education offerings **2**

Introduction **2**

Suggested training paths for zSecure job roles **3**

Central Security Administrator 3

Auditor / Compliance Officer 4

Decentralized Local Security Administrator 5

Limited Local Security Administrator 6

Customization, or on-site zSecure education **6**

Contact Information **6**

Standard IBM Security zSecure course offerings **7**

TK264G: IBM Security zSecure Admin Basic Administration and Reporting 7

TK254G: IBM Security zSecure RACF Management Workshop 10

TK244G: IBM Security zSecure RACF and SMF Auditing 12

TK224G: IBM Security zSecure UNIX System Services (USS) Security Overview 14

TK234G: IBM Security zSecure CARLa Auditing and Reporting Language 16

TK274G: IBM Security zSecure Audit Rule-based Compliance Evaluation and Customization 18

IBM Security zSecure education offerings

Introduction

This document contains an overview of the standard IBM Security zSecure courses that IBM can deliver for customers under the label of zSecure Lab Services.

Each zSecure course assumes that the attending students possess a basic knowledge of, and experience with, z/OS, TSO, and RACF. Where applicable, per zSecure course, the detailed course description mentions the expected knowledge and experience for students in the Prerequisites section. Here, you can also find the suggested zSecure and other courses that students can attend to obtain the expected prerequisite knowledge.

For convenience, zSecure courses are categorized by experience level: Basic, Intermediate, or Advanced. The following table outlines these zSecure course levels, explains the zSecure student experience that is expected, and outlines which course codes are assigned to each level.

Course level	**zSecure Experience**	**Course Code**
Basic	Basic level zSecure courses are targeted to be attended by the staff of new zSecure customers. No prior zSecure knowledge or experience is expected from the students to attend a basic training. However, students must have a working knowledge of RACF and have some basic experience with logging on to TSO and using ISPF panels and commands.	TK264G TK254G
Intermediate	Intermediate level zSecure courses expect that students are already familiar with the zSecure ISPF interface and know how to navigate through the various zSecure panels to select appropriate input sets, generate commands, or reports. Students must also know how to use overtyping and line commands to generate reports or profile maintenance commands. Generally, the students have 6 months or more experience with using zSecure Admin or Audit.	TK244G TK224G
Advanced	Advanced level zSecure courses are targeted for users that have a thorough knowledge of, and experience with, the standard zSecure ISPF interface. By attending advanced zSecure courses, students learn how they can customize reports or standard functions to fit with their company's needs. Students also learn how to automate certain standard functions and build their own reports, compliance rules, or standards that zSecure does not support out-of-the-box. It is suggested that students have at least 1 year experience with using zSecure Admin or Audit before attending an advanced level zSecure course.	TK234G TK274G

For zSecure users, the following job roles are distinguished:

- Central Security Administrator
- Auditor / Compliance Officer
- Decentralized Local Security Administrator
- Limited Local Security Administrator

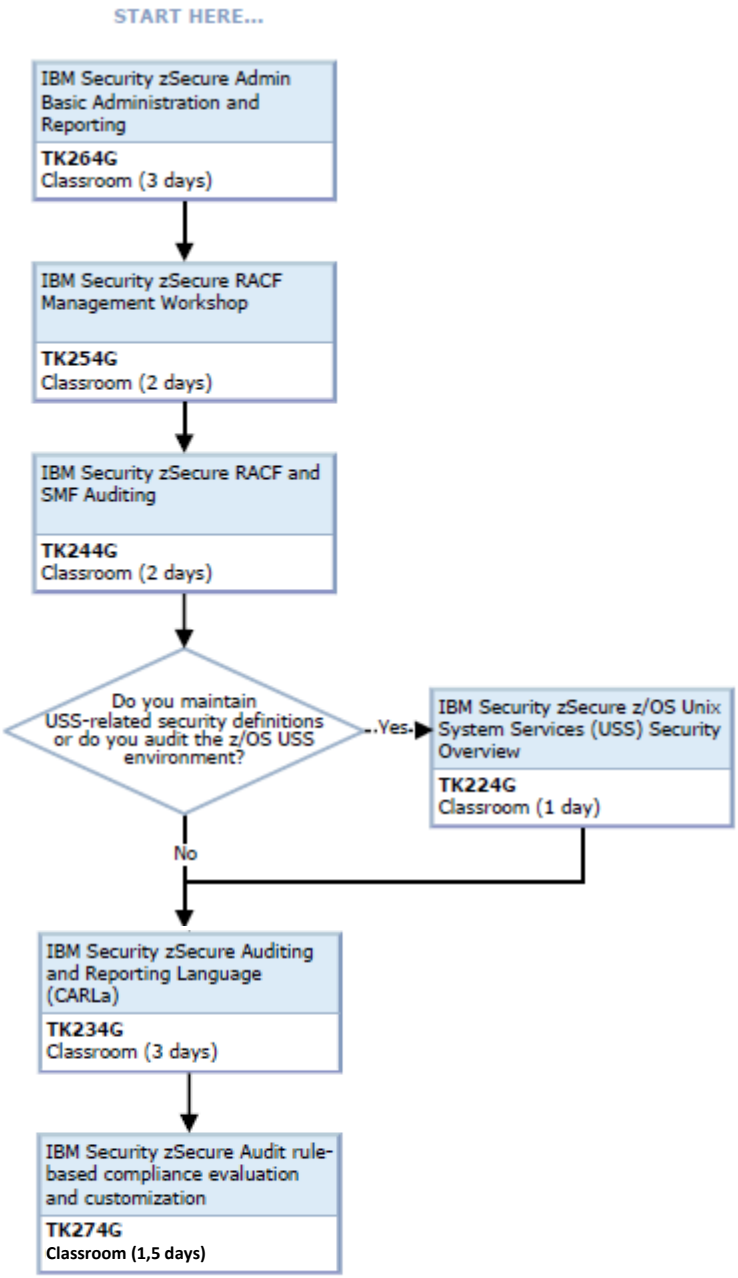
For each zSecure job role a zSecure training path is suggested. The next section of this document contains the role description for each zSecure job role and the suggested zSecure training courses that a user in that job role can attend.

Suggested training paths for zSecure job roles

Central Security Administrator

Role:

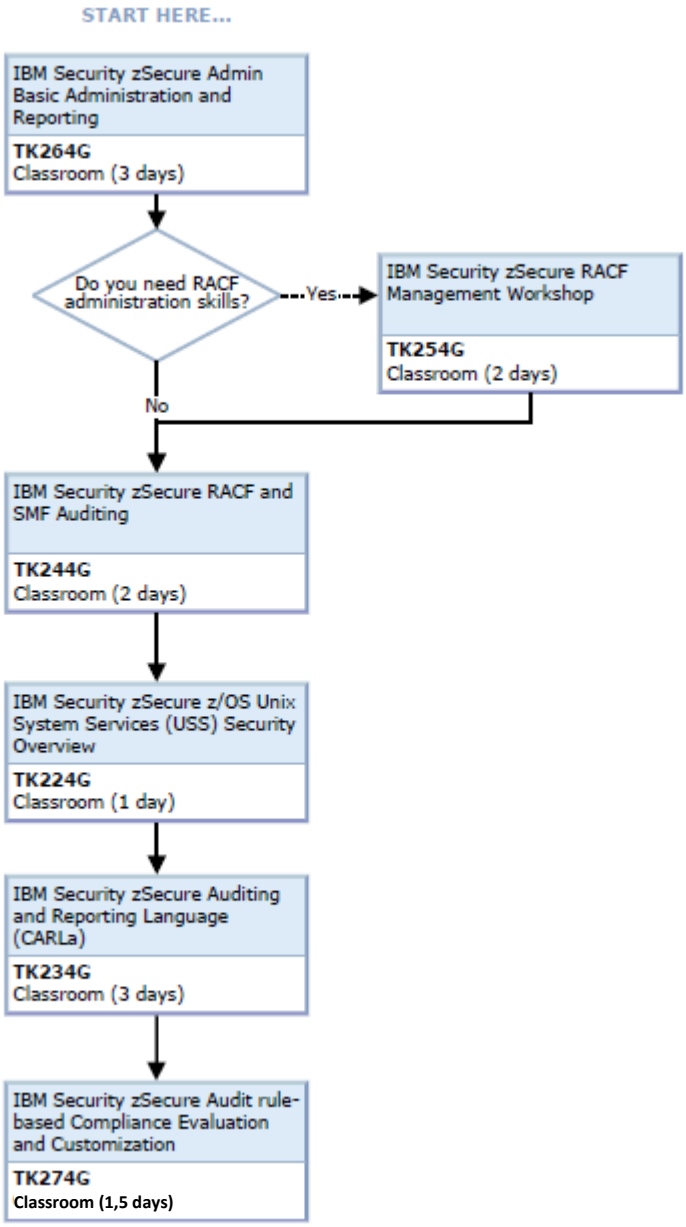
This job role includes those users with extensive RACF security administration capability, who are responsible for the system-wide administration of the RACF database. This job role includes the maintenance of the class descriptor table and the SETROPTS parameters. In addition, system programmers involved in the z/OS security process often require the same type of training as the Central Security Administrator.



Auditor / Compliance Officer

Role:

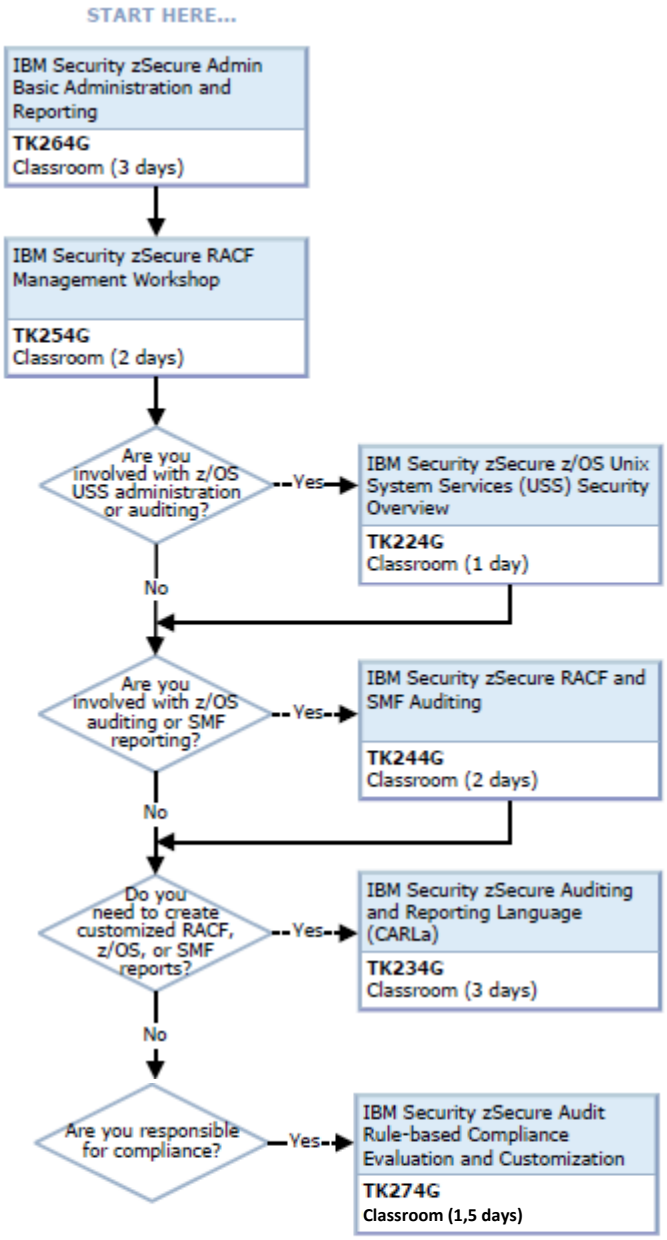
This job role includes the central or decentralized employees who are responsible for auditing security implementation on the z/OS system and running rule-based compliance evaluations.



Decentralized Local Security Administrator

Role:

This job role includes local or decentralized employees with extensive RACF security administration capabilities. In addition to their basic security administration tasks, they often define, maintain, and delete user, group, dataset, and general resource profiles. They also administer the access control lists of resource profiles within their scope.

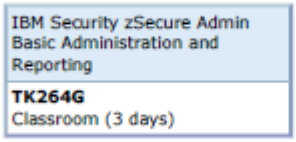


Limited Local Security Administrator

Role:

In general, the term Limited Local Security Administrators is used for personnel that are assigned limited RACF administrative capabilities. Usually, they are responsible for executing basic security administrative tasks such as resetting passwords, resuming users, and adding (or removing) existing users to (from) existing groups. Typical examples of limited local security administrators are non-technical staff, helpdesk, or first-line support staff.

START HERE...



Customization, or on-site zSecure education

All zSecure training courses can be customized to fit with the training requirements, current use, and experience of the involved customer(s). When a customer prefers, zSecure courses can be delivered on-site.

IBM can provide dedicated zSecure education systems that can be used to host zSecure courses at a fixed rate per course day. Alternatively, customers can elect to use their own z/OS Test / Education system to host zSecure courses at no additional charge.

Pricing of customized and on-site zSecure education sessions depends on the following factors:

- Duration of the course(s). IBM charges a fixed day/hour rate for the zSecure instructor.
- IBM charges a fixed rate of € 400 per half day of instructor travel time.
- The use of the IBM supplied IRLP z/OS education system to host a course is charged at a flat rate per course day.
- When applicable, the time, of the zSecure Enablement specialist to customize a course or write additional content that is not part of a standard training offering, is charged at a fixed rate per hour.
- Travel and expenses (flights, hotel, visa application, rental car, public transportation, meals, etc.) for the zSecure instructor are charged based on the costs that occur.
- An electronic copy of zSecure course materials is included in the standard pricing. If required by the customer, printed copies can be provided and shipped based on actual costs. However, when preferred, customers are authorized to print their own hard copies of the zSecure course guides.

Contact Information

For more questions, comments, and cost estimates for customized or on-site training zSecure education, you can contact our zSecure Enablement specialist.

Tom Zeehandelaar

IBM Security zSecure Development

Email: tom.zeehandelaar@nl.ibm.com

Phone: +31 (0)6 43351728

Standard IBM Security zSecure course offerings

In this section of the document, you find the detailed description of all standard zSecure course offerings. Each standard zSecure course description includes the following information:

- Course code and title
- Recommended course duration in days
- Skill level indication
- Objectives
- Intended audience
- Prerequisites
- Outline / Agenda

TK264G: IBM Security zSecure Admin Basic Administration and Reporting

Overview

Recommended duration: 3 Days

Skill level: Basic

This course is an instructor-led course that provides basic introduction of the IBM Security zSecure Admin ISPF interface for customers who administer RACF profiles and generate basic RACF overview reports.

This course focuses on frequently used administrative functions, standard reports, and verification functions of IBM Security zSecure Admin. Gain experience in administering RACF profiles using the built-in functions and line commands that the zSecure ISPF interface provides. Learn how to report and review RACF profiles using the built-in functions and supported line commands. Verification functions that report RACF database inconsistencies are explored and demonstrated. The zSecure-specific CKGRACF function is described and explained. Finally, you also learn how to produce customized reports, tailor the RACF installation data field, and define company-specific custom fields. Hands-on exercises are included in each course unit.

Objectives:

- Introduce the IBM Security zSecure Admin tool
- Select and review RACF profiles with the ISPF zSecure Admin panels and examine access control lists (ACLs) for resource profiles
- Perform profile maintenance and use supported features to apply bulk changes
- Review and maintain RACF SETROPTS options, Class Descriptor table (CDT) settings, and maintain input sets to control your IBM Security zSecure Admin session
- Show changes for the same system over time or differences between different systems
- Use the standard reports that IBM Security zSecure Admin provides
- Produce user and group profile reports and compare users or groups side-by-side
- Produce resource reports about various resources and defined access
- Use the Verify options to report and resolve RACF database inconsistencies, and learn about CKGRACF
- Define custom reports, customize Installation data, and define RACF custom fields

Audience:

This basic-level course is intended for RACF administrators who use the IBM Security zSecure Admin ISPF panel interface. It is also suitable for RACF administrators, auditors, and compliance officers who use the IBM Security zSecure Admin ISPF panel interface, the built-in functions, and commands to review and report about RACF profiles.

Prerequisites:

Before taking this course, make sure that you have a working knowledge of RACF. It is also recommended you have the following skills:

- The ability to log on to TSO
- Use ISPF panels to navigate TSO menus, use options, and run commands to view and manipulate output results

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

- An Introduction to the z/OS Environment ES05G
- z/OS JCL and Utilities ES07G
- Fundamental System Skills in z/OS ES10G
- IBM z/OS Bootcamp ESZ0G
- z/OS System Operators ES27G
- z/OS Facilities ES15G
- Basics of z/OS RACF Administration ES19G
- Effective RACF Administration BE87G

Course outline/agenda:

Run IBM Security zSecure Admin

- List the advantages of using IBM Security zSecure Admin to administer RACF
- Identify the input sources of information that IBM Security zSecure Admin uses
- Select different input sources
- Use the basic Setup panels to define and maintain input sets and configure or change the zSecure Admin run options

Select and display existing RACF profiles

- Use the zSecure Admin ISPF interface for RACF profile selection
- Select and display details of user profiles that match selection criteria
- Select and display details of group profiles that match selection criteria
- Select and display details of dataset profiles that match selection criteria
- View and sort the access control lists (ACLs) in different formats
- Select and display details of general resource profiles that match selection criteria

Perform profile maintenance

- Modify single profiles using line commands, overtyping commands, or the Quick User Administration panel
- Display and manage application segments
- Change profiles that affect multiple profiles and generate multiple RACF commands
- Update, define, delete, or recreate up to 10 profiles of the same entity with the Mass Update function
- Perform bulk changes with the FORALL function

Use advanced options

- Display SETROPTS and Class Descriptor Table settings
- Define new data sets to serve as input to zSecure
- Use the Show differences function to report changes of system settings and profiles

Produce RACF administration reports

- Produce reports about RACF profiles and resources
- Report and review the group tree of a RACF database
- Produce USERDATA and other standard reports
- Produce general status and system settings reports
- Report who can manage application segments

Create specific user and group reports

- Produce reports about users based on password or password phrase characteristics
- Identify users with specific attributes
- Report groups and their settings
- Compare different users and groups side-by-side to identify different connections and permissions

Create resource reports

- Identify the sensitive resources and global writable data
- Select and report general resources including their member lists
- Produce reports about Global Access Checking (GAC) tables and started tasks
- Report the status of digital certificates

Produce RACF management reports

- Identify inconsistencies in the RACF database
- Decide how to fix these inconsistencies
- Name the distinct features of the CKGRACF component
- Select and generate CKGRACF commands

Create customized reports

- Create your own customized reports
- Customize the way that zSecure Admin prints and displays RACF installation data
- Define and maintain RACF custom fields

TK254G: IBM Security zSecure RACF Management Workshop

Overview

Recommended duration: 2 Days

Skill level: Basic

In this workshop, you learn how to maintain a Resource Access Control Facility (RACF®) database with IBM® Security zSecure Admin. Also, you learn how to monitor the system with IBM Security zSecure Audit. In the included hands-on exercises, you act as the hypothetical RACF security administrator of the imaginary PMI Company. In this job role, you are responsible for the definition of a RACF security environment for a specific department within the PMI Corporation. You learn the basics of the security administration process and how to translate company security policies and guidelines into specific RACF profile definitions and settings. You also learn how to verify the quality and validity of the RACF profiles that you define. Finally, you learn how to interpret and report SMF events that are logged on the z/OS system during this workshop. You spent the RACF management workshop time on the completion of the exercises at your own pace. The instructor assists and explains when this assistance is needed.

Objectives:

- Describe the purpose and flow of the RACF management workshop
- Set up a flexible RACF group structure for a department based on PMI security policies and IT guidelines
- Define a departmental security administrator user ID, user IDs for plot writers, verify password quality, and create and refresh an IBM Security zSecure CKFREEZE data set
- Create role-based function groups, resource profiles, and create an IBM Security zSecure UNLOAD data set
- Implement role-based access using connections and permissions to the function groups
- Use and explain the various zSecure Admin Verify functions, define a started task, verify started procedures, and manage staff member changes
- Review and, if applicable, maintain RACF audit settings and report and examine SMF records that are logged during the workshop
- Prevent users with the OPERATIONS attribute from accessing your PMI departmental data sets
- Clean up RACF profiles and, if applicable, data sets, and catalog aliases

Audience:

This basic-level RACF management workshop is intended for users that are responsible for the management of, and reporting about, profiles and authorities in RACF. For example: security administrators, compliance officers, systems programmers, and potentially also auditors.

Prerequisites:

You should have:

- Basic knowledge of, **and** experience with, RACF
- Familiarity with the IBM Security zSecure Admin **or** Audit ISPF panel interface

When you do not have these skills, you can learn these skills by attending one or more of the following suggested courses:

- Basics of z/OS RACF Administration ES19G
- Effective RACF Administration BE87G
- IBM Security zSecure Basic Administration and Reporting TK264G

Course outline/agenda:

- Workshop and case introduction
- Set up group profiles for your department
- Create a security administrator user ID and plot writer user IDs
- Create and refresh IBM Security zSecure Admin UNLOAD and CKFREEZE data sets
- Maintain RACF user and group profiles
- Implement role-based access using function groups
- Define, maintain, and examine RACF dataset profiles
- Use and explain the working of Verify functions; Protect all, All not empty, and Password
- Define and verify started procedures
- Review and, if applicable, maintain RACF audit settings
- Report and examine SMF records that are recorded during the workshop
- Clean up RACF profiles and, if applicable, data sets, and catalog aliases

TK244G: IBM Security zSecure RACF and SMF Auditing

Overview

Recommended duration: 2 Days

Skill level: Intermediate

This course describes the audit concerns that IBM® Security zSecure™ Audit reports. The course explains how to audit the content of your Resource Access Control Facility (RACF®) database and the z/OS sub systems such as CICS, IMS, and DB2. You can measure your current security and z/OS system settings against the security requirements of a selected policy level. Furthermore, you learn how to review the current general System Management Facility (SMF) and RACF audit settings. This course also explains how to use and interpret the predefined SMF audit reports, and how to create your own customized SMF reports. In addition, you learn about using Access Monitor data sets containing statistics about historic RACF decisions. These ACCESS data sets can be used to find profiles, permissions, or connections that are not used and can, therefore, be removed from the RACF database. Finally, the concepts of the library and sequential data set status and change analysis functions are explained and demonstrated.

Objectives:

- 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

Audience:

This intermediate-level 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. These job roles use the IBM Security zSecure Audit and Admin ISPF panel interface, the built-in functions, and commands to review and report about RACF profiles. RACF and z/OS compliance officers might also benefit from attending this training.

Prerequisites:

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 TK264G
- Basics of z/OS RACF Administration ES19G
- Effective RACF Administration BE87G

Course outline/agenda:

Unit 1: Introduction to RACF auditing

- List the RACF resources that must be audited
- Generate and interpret an audit concerns report
- Identify all the profiles that a particular user ID owns
- Identify the user IDs that are authorized to maintain RACF application segments

Unit 2: Auditing user IDs and passwords

- Generate and interpret user ID reports
- Identify last logon and password / password phrase aging
- Identify user IDs are assigned system-wide or group-specific authorities
- Generate and interpret a report of trusted user IDs

Unit 3: Auditing sensitive resources

- Identify sensitive profiles and the user IDs that are authorized to modify them
- Identify user IDs that can create profiles of various types
- Audit started tasks and programs

Unit 4: Audit subsystems

- Explain how to gather the subsystem audit information
- Generate CICS and IMS audit reports about regions, transactions, programs, and program specification blocks
- Generate DB2 audit reports about various DB2 resource types and use DB2-specific ACLs

Unit 5: Generate SMF audit reports

- Explain the concepts of SMF auditing
- Report the events that are logged in SMF
- Select events that are logged in SMF with the ISPF interface
- Use predefined reports to report about SMF events
- Create customized SMF reports

Unit 6: Access Monitor and RACF-Offline

- Explain the access monitor functions and reports
- Produce access summary overview reports
- Compare historic access events against current allocated RACF database definitions
- Analyze permit, connect, and profile usage to remove unused profiles and authorizations
- Explain the function of the RACF-Offline component and recognize when using RACF-Offline is beneficial

Unit 7: Library Analysis

- Track changes that occur in z/OS system sensitive libraries or sequential data sets

TK224G: IBM Security zSecure UNIX System Services (USS) Security Overview

Overview

Recommended duration: 1 Day

Skill level: Intermediate

This course describes the security-related aspects of a z/OS UNIX System Services (USS) environment. Learn USS concepts, followed by an overview of the USS-related functions and features of the IBM Security zSecure Admin and Audit products. Using the zSecure built-in reports and standard interface, you learn how to obtain USS-related information from RACF profiles and review the contents of the USS reports. Audit recommendations and the RACF audit concerns that are applicable to a z/OS USS environment are described. In addition, you learn about the USS-related resource profiles in the FACILITY and UNIXPRIV classes.

Objectives:

- Describe the authorization checking process to access a UNIX file or directory
- Create the appropriate RACF definitions to define a z/OS UNIX System Services user ID
- Describe the audit options for z/OS UNIX System Services
- Set up permissions to control access to a file or directory
- List and maintain extended access control list (ACL) entries
- List and maintain the audit settings for a file or directory

Audience:

This intermediate-level course is intended for users that are involved in defining and maintaining USS-related security definitions or auditing the z/OS USS environment. For example: security administrators, compliance officers, system programmers, and auditors.

Prerequisites:

You should have:

- Basic knowledge of, **and** experience with, RACF
- Familiarity with the IBM Security zSecure Admin or Audit ISPF panel interface

If you do not have these skills, you can learn these skills by attending one or more of the following suggested courses:

- Basics of z/OS RACF Administration ES19G
- Effective RACF Administration BE87G
- IBM Security zSecure Admin Basic Administration and Reporting TK264G
- IBM Security zSecure RACF and SMF auditing TK244G

Course outline/agenda:

Unit 1: z/OS UNIX System Services (USS) security concepts

- Describe the z/OS UNIX System Services identification and authentication process
- Describe the various USS processes, resources, attributes, and reports
- Secure USS daemons and servers

Unit 2: Protect files and directories

- Report and maintain the fields in the file security packet (FSP)
- List and modify USS extended file attributes and object access checking
- Secure USS files and directories with extended access control lists (ACLs)
- Report files and directories that have extended ACL entries with zSecure

Unit 3: Reporting and auditing in a USS environment

- Report about shared and empty UID and GID values
- Generate extended program attributes reports
- Explain HFS and zFS auditing concepts
- Use and inspect the USS-related RACF profiles
- Avoid common HFS or zFS audit RACF pitfalls
- Generate reports about trust reasons in USS
- Audit daemons and servers
- Generate reports about USS-related SMF records

TK234G: IBM Security zSecure CARLa Auditing and Reporting Language

Overview

Recommended duration: 3 Days

Skill level: Advanced

Learn the basics of the IBM Security zSecure programming language CARLa. This course teaches you to use the CARLa Auditing and Reporting programming language to create reports for RACF, SMF, UNIX Systems Services (USS), CICS, DB2, and RACF command generation. Approximately 40 percent of the course is spent on hands-on lab exercises, where you produce CARLa code that can be used for effective management and reporting on RACF, SMF, USS, CICS, and DB2. You also learn to use the CARLa programming language to create your own reports and commands or modify existing zSecure RACF functions to fit with your company's requirements. In addition, you learn how to automate these functions by using them in scheduled batch jobs. Furthermore, you learn how to use CARLa to produce your own reports, emails, CARLa programs, or commands.

Objectives:

- Use the CARLa interface to process the allocated supported input sources and introduction of the main CARLa statements
- Use various SELECT options for input filtering and to specify output formatting using the SORTLIST statement and output modifiers
- Apply CARLa frequently used functions such as subselect, lookup, substring, parsing, and using the DISPLAY statement
- Define report titles, redirect output, add statistics with the SUMMARY statement, and use CARLa to generate RACF commands
- Process multiple input sources simultaneously, generate CARLa code with 2-pass CARLa, and use the CARLa compare options
- Use CARLa in batch jobs to automate the generation of reports, CARLa code, RACF commands, emails, WTO messages, and XML-formatted output
- Generate reports about the various logged SMF records
- Learn about and use other supported CARLa NEWLIST types

Audience:

This advanced-level course is for security administrators, systems programmers, compliance officers, and auditors who want to create their own reports or generate automated RACF or USS commands with the IBM Security zSecure CARLa Auditing and Reporting Language (CARLa).

Prerequisites:

You should have:

- Basic knowledge of, **and** experience with, RACF
- Familiarity with the IBM Security zSecure Admin **or** Audit ISPF panel interface

When you do not have these skills, you can learn these skills by attending one or more of the following suggested courses:

- Basics of z/OS RACF Administration ES19G
- Effective RACF Administration BE87G
- IBM Security zSecure Basic Administration and Reporting TK264G
- IBM Security zSecure RACF Administration Workshop TK254G
- IBM Security zSecure RACF and SMF auditing TK244G

Course outline/agenda:

Unit 1: Introduction and the CARLa Interface

- The information types that CARLa can process.
- Run CARLa programs using Interactive System Productivity Facility (ISPF)
- Three most used CARLa keywords
- Write your own customized CARLa reports

Unit 2: CARLa SELECT and SORTLIST statements

- Produce customized RACF reports
- Specify the profiles that you want to report with SELECT statements
- Format reports with SORTLIST statements and output modifiers
- Add custom values to reports with user-defined fields

Unit 3: Frequently Used CARLa functions

- Report about information that is stored in repeat groups
- Sub-filter the repeat group entries with SUBSELECT statement
- Create ISPF reports with drill-down capability using a DISPLAY statement
- Combine information from multiple profiles and segments
- Use string processing in reports

Unit 4: NEWLIST and SUMMARY options

- Combine multiple reports with the NEWLIST statement
- Add statistical information to reports
- Generate RACF commands with CARLa

Unit 5: Advanced CARLa Functions

- Use profile or record pre-selection with PROFLIST function
- Use multiple input files to report about multiple systems or changes over time for the same system
- Write multiple-pass CARLa programs to solve more complex problems / challenges

Unit 6: Use CARLa in batch jobs

- Run CARLa programs with Job Control Language (JCL)
- E-mail reports that CARLa generates
- Generate Write To Operator (WTO) messages with CARLa
- Produce reports in Extensible Markup Language (XML) format

Unit 7: SMF reporting with CARLa

- Produce reports about events that are logged in SMF records

Unit 8: Other supported CARLa NEWLIST types

- Produce and customize trusted users report
- Report information from the Class Descriptor Table (CDT) with CARLa
- Report the global RACF options (SETROPTS) with CARLa
- Produce reports about the scope of a user's permissions
- Report custom CONSOLE class and DB2 region reports

TK274G: IBM Security zSecure Audit Rule-based Compliance Evaluation and Customization

Overview

Recommended duration: 1,5 Days

Skill level: Advanced

This course introduces the IBM Security zSecure Audit rule-based compliance evaluation framework.

The course discusses rule-based compliance evaluation concepts and includes an overview and demonstration of the supported compliance functions and reports. With the standard built-in compliance evaluation interface, you report the compliance of your systems against one or more of the supported external standards: STIG, GSD, PCI-DSS, or zSecure extra.

The course teaches you how to customize the compliance evaluation for the supported standards to fit with your company's requirements. Finally, you learn how to create a company-defined compliance standard.

Hands-on exercises are included to enforce the skills that are taught in this course so that you can experiment with the rule-based compliance evaluation interface.

Objectives:

- Explain the concept of rule-based compliance evaluation with zSecure Audit
- Run compliance evaluations against the supported standards GSD331, STIG, and PCI-DSS
- Use the compliance evaluation results to apply the applicable changes to comply with the selected external compliance standard
- Customize compliance evaluations to fit with company security and audit policies
- Build customized system-defined compliance standards, rule sets, rules, and tests

Audience:

The target audience for this advanced level course is security administrators, auditors, and compliance officers.

Prerequisites:

You should have the following skills:

- Basic knowledge of **and** experience with z/OS **and** RACF
- Familiarity with the IBM Security zSecure Audit ISPF panel interface
- Knowledge of **and** experience with the CARLa programming language

These skills can be obtained by attending the following courses:

- IBM Security zSecure RACF and SMF Auditing TK244G
- IBM Security zSecure CARLa Audit and Reporting Language TK234G

Course outline/agenda:

Unit 1: Rule-based compliance introduction and concepts

- Explain the concept of the compliance evaluation framework
- Name the supported external standards
- Introduce the concept and CARLa syntax of compliance standards, domains, rule sets, rules, and tests
- Describe the input sources that the compliance evaluation framework uses
- Review, populate, and maintain the CKACUST, CKACUSV, and assertion data sets

Unit 2: Running compliance evaluations and interpret the results

- Run rule-based compliance evaluations against the supported standards with the zSecure Audit compliance evaluation interface
- Understand and explain the result of compliance evaluations
- Determine the appropriate action(s) to take for your system to become compliant
- Define or select a subset of rule sets for running a compliance evaluation against
- Run compliance evaluations for multiple complexes simultaneously

Unit 3: Customizing compliance standards, rules, and tests

- Customize the predefined rule sets, rules, and tests to fit the company policies
- Suppress rules that do not apply to your company
- Build company-specific rule sets, rules, and tests