

□

IBM Security zSecure UNIX System Services (USS) Security Overview
Information

Length:	1.0 Day
__Ref:	TK223G-X
Delivery method:	ClassroomInstructor Led Online
Price:	EUR

Overview

In this workshop, you learn to maintain a RACF® database with IBM® Security zSecure®, Admin and monitor the system with IBM Security zSecure Audit. During hands-on exercises, you act as a RACF security administrator for a fictitious company. In this simulated job role, you learn to define a RACF security environment for a specific department.

This workshop teaches the basics of the security administration process and how to implement company security policies and guidelines into specific RACF profile definitions and settings. You learn to verify the quality and validity of RACF profiles that you define. Finally, you learn to interpret and report SMF events that the z/OS® system logs during this RACF management workshop.

Public

This intermediate-level course is intended for users that are involved with the maintenance of USS-related security definitions or auditing of the z/OS USS environment. For example, security administrators, compliance officers, systems programmers, and auditors can benefit from taking this course.

Prerequisites

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

- * 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:

- ES19G Basics of z/OS RACF Administration
- BE87G Effective RACF Administration
- TK263 IBM Security zSecure Admin Basic Administration and Reporting
- TK243 IBM Security zSecure RACF and SMF auditing

Objective

- 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

Topics

Unit 1: UNIX System Services security introduction

Unit 2: Protect files and directories

Unit 3: Report and audit UNIX System Services

□