



BMC Mainframe: zSecure Suite Level 1 - Foundation Skills

COURSE ABSTRACT

COURSE CODE

» MGRS-ZSSF-2021

APPLICABLE VERSIONS

» Not Applicable

DELIVERY METHOD

» Instructor-led Training (ILT)

COURSE DURATION

» 5 Days

PREREQUISITES

- » Attendees should have thorough working knowledge of RACF
- » BMC Mainframe: RACF Administration & Auditing

RECOMMENDED TRAININGS

» NA

Course Overview

The course is developed and delivered by © RSM Technology.

This zSecure foundation level course is designed, written, and presented by RACF & zSecure specialists. The course introduces and explains the essential elements of zSecure, focusing on zSecure Admin, zSecure reporting and SMF auditing.

This is a hands-on course, in which attendees will learn to perform the frequently used administrative functions, standard reports, and verification functions of IBM Security zSecure Admin. Students will also learn how to audit the content of their RACF database and z/OS system, and to measure the results against the security requirements of a selected policy level. In addition, the course teaches how to review the current general SMF & RACF audit settings and interpret the pre-defined SMF audit reports. Attendees will also be shown how to create their own customized SMF reports.

Target Audience

The course is suitable for RACF Administrators responsible for RACF Administration at their installation.

Learner Objectives

- » Display RACF users and user information from the ISPF zSecure Admin panels
- » Manage RACF groups interactively and create printed reports
- » Administer RACF dataset and general resource profiles and examine access lists
- » Create textual reports on RACF users, groups, data sets, and general resources
- » Review and maintain RACF and Class Descriptor Table (CDT) options
- » Define and maintain input files to control your IBM Security zSecure Admin session
- » Use the reports provided with IBM Security zSecure Admin
- » Analyze RACF profiles containing segments
- » Review the installation's RACF control tables and analyze the group structure in the installation
- » Create reports on the RACF database and resolve inconsistencies
- » Customize installation data, compare users, queue commands, and run commands using CKGRACF
- » Describe the flow of a security call from Resource Managers to RACF
- » Perform user and password audit analysis
- » Use the Audit functions to report on sensitive users and z/OS resources
- » Create Audit reports on key RACF and z/OS system table
- » Review the system-wide Audit settings
- » Select and process predefined SMF reports
- » Define custom SMF reports

BMC, BMC Software, and the BMC Software logo are the exclusive properties of BMC Software, Inc., are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other BMC trademarks, service marks, and logos may be registered or pending registration in the U.S. or in other countries. All other trademarks or registered trademarks are the property of their respective owners. ©2021 BMC Software, Inc. All rights reserved.



BMC Mainframe: zSecure Suite Level 1 - Foundation Skills

COURSE ABSTRACT

COURSE ACTIVITIES

- » Classroom Presentations
- » Demonstration


BMC MAINFRAME INFRASTRUCTURE AND PLATFORMS LEARNING PATH

- » <https://www.bmc.com/education/courses/find-courses.html#filter/%7B%22type%22%3A%22edu-specific-types-159150236%22%7D>

CERTIFICATION PATHS

- » This course is not part of a BMC Certification Path.

DISCOUNT OPTIONS

- » Have multiple students? Contact us to discuss hosting a private class for your organization
- » [Contact us for additional information](#) 

Course Modules

RACF Review

- » Introduction to RACF auditing
- » RACF review
- » Main RACF - z/OS components
- » How does RACF work?
- » RACF database structure
- » RACF profiles
- » Group profiles
- » User profiles
- » Dataset profiles
- » General resource profiles
- » Resource classes
- » Class Descriptor Table (CDT)
- » Macro ICHRRCODE or CDT profiles
- » Adding new dynamic General Resource classes
- » Static to dynamic CDT migration
- » The RACF interface
- » Calling RACF
- » RACF router table
- » RACF as a database manager
- » Separation of functions
- » Summary

Running IBM Security zSecure Admin

- » zSecure Admin
- » RACF management tool
- » RACF information sources
- » RACF databases
- » CKFREEZE information
- » IBM Security zSecure Collect
- » Information sources access
- » Restricted view
- » Results
- » Using IBM Security zSecure Admin
- » Selecting input files
- » The Setup menu
- » The Setup files
- » Selecting Setup files
- » Summary

Selecting & Displaying Existing RACF Profiles

- » Basic administration functions
- » Functional approach management
- » Profile type selection
- » Profile subset selection
- » Selecting user profiles
- » Advanced criteria

- » Other fields
- » Attributes
- » Segment presence or absence
- » Segment presence detailed selection
- » Output/run options
- » Results in ISPF format
- » Viewing additional user fields
- » User profile line commands
- » Detailed user information
- » More user information
- » Show all relevant user information
- » Print full page user report
- » Selecting group profiles
- » Additional criteria
- » Profile fields
- » Connect fields
- » Group profile line commands
- » Additional group information
- » Selecting dataset profiles
- » Additional criteria
- » Profile fields
- » Access list
- » Selected dataset profiles
- » Dataset profile line commands

BMC, BMC Software, and the BMC Software logo are the exclusive properties of BMC Software, Inc., are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other BMC trademarks, service marks, and logos may be registered or pending registration in the U.S. or in other countries. All other trademarks or registered trademarks are the property of their respective owners. ©2021 BMC Software, Inc. All rights reserved.



BMC Mainframe: zSecure Suite Level 1 - Foundation Skills

COURSE ABSTRACT

- » Detailed dataset information
- » Access Control Lists (ACLs)
- » ACL display formats
- » ACL order
- » ACL default display
- » ACL Explode
- » ACL Resolve
- » ACL - sort by access
- » Selecting general resource profiles
- » Additional criteria - Profile fields
- » Resource class list
- » General resource profiles in FACILITY class
- » General resource profile line commands
- » Additional general resource information
- » Summary

Profile Maintenance

- » Actions on a single profile
- » Running line commands
- » Managing logon information
- » The generated RACF command
- » Command generation
- » CKGRACF
- » Setup for command generation
- » Connect
- » Select user ID or group
- » Line command
- » Command execution
- » The C line command
- » The Copy connect panel
- » Adding ACL entries
- » Managing ACL entries
- » General resource ACLs
- » Modifying ACL members
- » Running the generated commands
- » Quick user administration
- » Modifications using quick user administration
- » Multiple RACF commands
- » Copying user IDs
- » The User copy panel
- » Commands generated to copy user ID
- » The Results panel

- » Command results
- » Running the commands
- » Viewing the results
- » Verify successful command execution
- » Deleting user IDs
- » The User Delete panel
- » User ID deletion commands
- » Manage TSO information for a user ID
- » Manage user ID TSO information commands
- » Recreate a user profile
- » Managing multiple profiles
- » Mass update
- » User Multiple Copy
- » Managing application segments
- » Summary

Advanced Options

- » SETROPTS and class settings
- » Review and change current settings
- » Review and maintain SETROPTS
- » Review or maintain CDT settings
- » Show line commands for CDT settings
- » Review or maintain class details
- » Application configuration
- » The Setup menu
- » Run options
- » Define a new set
- » Define a new set using existing datasets
- » Specify input dataset type
- » Optionally assign NJE node or system name
- » Define a new set using new datasets
- » Allocate space for new UNLOAD or CKFREEZE
- » Summary

RACF Administration Reports

- » The Reporting RACF and resources
- » Reporting
- » Profiles
- » Profiles and datasets
- » Non-redundant profiles
- » Redundant profiles

- » Scope/Permit
- » User ID or group access
- » Match profiles
- » Match profiles selection display
- » View the RACF database Group Tree
- » Reporting
- » Group Tree: selection, report, report details
- » Report USERDATA and other miscellaneous reports
- » Reporting
- » USERDATA
- » USERDATA details
- » Managing USERDATA
- » Reporting
- » Selected reports: examples, details
- » General Status and System Settings reports
- » Report profiles and segments
- » Profiles and segment reports
- » Display RACF control tables, select reports
- » Display the SETROPTS settings
- » Display RACF dataset names
- » Display the CDT settings, details
- » Report field-level access, access checking, checking profiles
- » Displaying a FIELD class profile
- » Summary

Specific Userid & Group Reports

- » Report user IDs based on password characteristics
- » Report RACF user ID population
- » User ID reports
- » Show user ID last logon overview summary (LGAGESUM)
- » Last logon older than five years (LGAGE5YR)
- » Show user IDs by password age summary (PWAGESUM))
- » User ID password age 2-3 years (PWAGE2YR)
- » User IDs with initial password (PWAGENEV)
- » User IDs with failed password attempts (PWTRIES)

BMC, BMC Software, and the BMC Software logo are the exclusive properties of BMC Software, Inc., are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other BMC trademarks, service marks, and logos may be registered or pending registration in the U.S. or in other countries. All other trademarks or registered trademarks are the property of their respective owners. ©2021 BMC Software, Inc. All rights reserved.



BMC Mainframe: zSecure Suite Level 1 - Foundation Skills

COURSE ABSTRACT

- » User IDs with non-expiring password (PWNNONE)
 - » User IDs using a password phrase
 - » Reporting user IDs by attribute
 - » User IDs with specific attributes
 - » User IDs with specific attributes
 - » User IDs with a specific attribute
 - » Specify attribute
 - » Review report
 - » User IDs with any attribute
 - » Selection
 - » User IDs with a system attribute (AUTHSYS)
 - » This report shows user IDs with a group attribute (AUTHGRP)
 - » User IDs with UID 0 (AUTHUID0)
 - » Group reports
 - » Select group profile fields
 - » Subgroups
 - » Display
 - » Report on group connect authority
 - » Selection
 - » Display
 - » Report scope of a user ID
 - » Specify exclusions
 - » Display
 - » Print format
 - » Group tree report
 - » Display
 - » Connected user IDs
 - » Comparing user IDs and groups
 - » Comparing user profiles
 - » Display permits
 - » Display connects
 - » Comparing group profiles
 - » Display permits
 - » Display permits details
 - » Summary
- Reporting Resource Profiles**
- » Identify sensitive resources and global writable data
 - » Report sensitive profiles
 - » Specification, Display, Detail
- » Global Writable datasets
 - » Display
 - » Global writable UNIX files
 - » Display
 - » Reporting member lists
 - » Members in multiple groups
 - » Merged member list
 - » Select profile fields
 - » Show merged member list option
 - » No, No display, No detail
 - » Yes, Yes display
 - » Duplicates
 - » Global Access Checking tables and started task reporting
 - » Global Access Checking tables
 - » Select profile
 - » Dataset detail
 - » Privileged and trusted started tasks
 - » Select statement
 - » Show segment
 - » Select task
 - » Detail
 - » No segment selection
 - » Sorted
 - » Reporting digital certificates
 - » Trusted only
 - » Detail
 - » CERTAUTH, SITE
 - » Trusted due to expire
 - » Summary
- RACF Management Reports**
- » RACF database inconsistencies
 - » RACF management
 - » Verify
 - » Verify panel
 - » Restrict scope of Verify functions
 - » Verify Permit: Orphan specification
 - » Verify User permit
 - » Verify On volume
 - » Verify (All) not empty
 - » Verify Program
 - » Verify Started task
- » CKGRACF the alternative way to access RACF
 - » RACF management: CKGRACF
 - » Types of CKGRACF queued commands
 - » Timed commands
 - » Timed commands: Diagram, Connect, Permit
 - » Select profiles with queued commands
 - » Line commands for queued commands
 - » Refresh queued commands
 - » Multiple- authority
 - » Line command
 - » Dual authority
 - » Change user password
 - » Run CKGRACF command
 - » List queued commands
 - » Action commands
 - » Review request command
 - » Password management
 - » Set default password
 - » Summary
- Customised Reports**
- » Customized reporting
 - » Custom report using standard output set
 - » Show standard select and display statement
 - » Adjust the selection criteria and display fields
 - » Customized user ID overview report
 - » Customized resource overview
 - » Customized STARTED report
 - » Customizing installation data
 - » Entities, Columns
 - » Customizing INSTDATA
 - » Overview display layout
 - » Detail display specification
 - » Customizing installation data
 - » Result
 - » Detail display
 - » Print layout
 - » RACF custom fields
 - » Defining new RACF custom fields

BMC, BMC Software, and the BMC Software logo are the exclusive properties of BMC Software, Inc., are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other BMC trademarks, service marks, and logos may be registered or pending registration in the U.S. or in other countries. All other trademarks or registered trademarks are the property of their respective owners. ©2021 BMC Software, Inc. All rights reserved.



BMC Mainframe: zSecure Suite Level 1 - Foundation Skills

COURSE ABSTRACT

- » Defining additional RACF custom fields
- » Activate newly defined RACF custom fields
- » Assigning values to custom fields: Add segment
- » Custom fields maintain values
- » Summary

zSecure Auditing

- » zSecure Audit Profiles reports
- » Audit concerns
- » Profiles and segments
- » Audit concerns
- » Display SETROPTS and CDT
- » Audit concerns control tables
- » Audit concern OVERVIEW details
- » Display the SETROPTS settings
- » SETROPTS audit concerns
- » Display RACF dataset names
- » Display Class Descriptor Table (CDT)
- » Display CDT details
- » Display the RACF router table
- » CDT and RACF router table consistency
- » Exercise 1.1
- » Select by Owner
- » Ownership by selected user
- » Ownership by any user
- » Displaying FIELD Class
- » Segments in profiles
- » Command Authority segments
- » FIELD class
- » FIELD class profile layout
- » FIELD- level access checking
- » Displaying a FIELD class profile
- » Practical exercise
- » Review questions
- » Summary

Auditing Users & Passwords

- » Introduction
- » Auditing the RACF user population
- » User reports
- » User last logon overview
- » Last user logon older than 4 years

- » Users by password age
- » User password age 3 to 4 years
- » Users with initial password
- » Users and invalid password attempts
- » Users with non-expiring password
- » Users with long password intervals
- » Users with weak passwords
- » Exercise 2.1
- » CARLa commands
- » SYSPRINT
- » ALU REVOKE
- » CKR2PASS
- » CKRCMD
- » Run ALU REVOKE
- » Results
- » Auditing highly authorized users
- » Users with attributes
- » Users with any system-wide attribute
- » Users with any group attribute
- » Users with UID equal to 0
- » Trusted users
- » Reason overview
- » Reasons detail overview
- » Reason details
- » Practical exercise
- » Review questions
- » Summary

Auditing Resources

- » Introduction
- » Auditing sensitive resources
- » Reports on profiles
- » Sensitive profiles
- » Sensitive data trustees
- » Sensitive data trustees – details
- » Trust reason
- » Trust reason details
- » Report sensitive profiles
- » Audit concern details
- » Practical exercise
- » Auditing create authorizations
- » Dataset create authority

- » Create authority for general resources
- » Report
- » Detail
- » Create authority for general resources in CARLa
- » Practical exercise
- » Auditing programs and started tasks
- » Programs
- » Authorized program reports
- » APF protected programs overview
- » APF protected program details
- » PADS programs
- » PADS overview
- » Started tasks
- » Report specifications
- » Started tasks overview
- » Started task details
- » Practical exercise
- » Review questions
- » Summary

SMF Auditing

- » Introduction
- » SMF audit specifications
- » Auditing
- » Who controls the audit settings?
- » System-wide specified audit settings
- » Profile-specified audit settings
- » Profile-level audit settings
- » Generating event reports
- » Investigating the system
- » System-wide audit settings
- » Resource class audit settings
- » Profile-level audit settings
- » SMF reporting
- » SMF reporting (cont.)
- » User events
- » User Action pane
- » User Attribute panel
- » Date and time panel
- » Data Set selection panel
- » HFS selection panel
- » Resource selection panel

BMC, BMC Software, and the BMC Software logo are the exclusive properties of BMC Software, Inc., are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other BMC trademarks, service marks, and logos may be registered or pending registration in the U.S. or in other countries. All other trademarks or registered trademarks are the property of their respective owners. ©2021 BMC Software, Inc. All rights reserved.



BMC Mainframe: zSecure Suite Level 1 - Foundation Skills

COURSE ABSTRACT

- » Db2 selection panel
- » User selection
- » Object selection
- » Event selection
- » SMF events caused by CRMBT users
- » RACF events – details
- » Non-RACF events – details
- » Practical exercise
- » Report RACF/CKGRACF- user commands
- » Report RACF/CKGRACF- user commands (cont.)
- » View RACF command details
- » Practical exercise
- » Predefined SMF reports
- » RACF exceptions report
- » Report the use of OPERATIONS: USEOPER report
- » Commands by SPECIAL users: CMDSPEC report
- » Command violations: CMDFAIL report
- » Dataset access violations: DSETVIOL report
- » UNIX (USS) violations: UNIXVIOL report
- » Violations and warnings by users - VWBYUSER report
- » Practical exercise
- » RACF events
- » All Events overview
- » All Events
- » - deleted resources
- » All Events - new group profiles
- » All Events - user changes
- » All Events - failed user changes
- » NOT NORMAL
- » NOT NORMAL – details
- » Commands
- » Practical exercise
- » SMF custom reports
- » Specifying fields
- » Additional options
- » SMF records
- » Profile changes
- » Summary of changes
- » Summary of commands
- » Custom events
- » More custom events
- » Event options
- » Display template
- » SMFDATA
- » Event details
- » Practical exercise
- » Review questions
- » Summary

Library Analysis

- » Introduction
- » Library analysis
- » How it works
- » Using library analysis
- » Purpose of library analysis
- » Identify differences
- » The audit - library menu
- » New CKFREEZE with signatures
- » CKFREEZE signature options
- » Library overview
- » Library changes report
- » Changes in load libraries
- » Changes in text libraries
- » Duplicate member analysis
- » Running duplicate member analysis
- » Duplicate members with different names
- » Duplicate members with identical names
- » Review questions
- » Summary

Question & Answer Session