BMC MAINFRAME INFRASTRUCTURE AND PLATFORMS

COURSE ABSTRACT

BMC Mainframe: RACF Security in a UNIX System Services Environment

COURSE CODE

- MGRS-RSUE-2021

APPLICABLE VERSIONS

- Not Applicable

DELIVERY METHOD

- Instructor-led Training (ILT)

COURSE DURATION

- 2 Days

PREREQUISITES

- BMC Mainframe: RACF Administration & Auditing
- Attendees should have a clear understanding of z/OS at a conceptual level and have an understanding of RACF.
- A familiarity with UNIX System Services and a knowledge of TSO/ISPF and JCL is also required.

RECOMMENDED TRAININGS

- NA

Course Overview

The course is developed and delivered by © RSM Technology.

Today it is vital that a System Z installation secures IBM's UNIX System Services (USS). Therefore, for Security Administrators and Systems Programmers working in a System z/USS environment, a sound understanding of how RACF works with USS is absolutely essential.

Designed, written and presented by specialist RACF consultants, this course introduces the USS RACF interface and describes and explains how RACF is utilized within the USS environment.

This course is regularly updated to reflect changes introduced up to (and including) the current releases of RACF and z/OS. In addition, there are now a number of challenging hands-on practical exercises included in the course.

Target Audience

The course is suitable for all Security Administrators and Systems Programmers working in a z/OS UNIX System Services environment.

Learner Objectives

- Describe the necessary requirements to implement a secure UNIX System Services environment
- Create users with OMVS segments and their resources
- Administer directory and file access using permission bits, ACLs and RACF classes
- List the RACF UNIX System Services General Resource Classes for Security
- Move around the UNIX System Services environment
- Use UNIX System Services commands with regards to security
- Use file systems and ACLs
- Recognize and understand USS error messages with regards to security
- Understand the security implications for Daemons and Servers
- Understand the use of superuser and UID(0)
- Recognize the tasks needed to audit USS Security events.

BMC Mainframe: RACF Security in a UNIX System Services Environment

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

Introduction to USS Features and Services

- What are 'Open Systems'?
- z/OS USS
- Benefits of USS
- z/OS USS components
- z/OS UNIX interfaces
- HFS
- SAF for z/OS UNIX
- USS security with RACF
- UNIX internals overview
- The Kernel
- LOADxx and the IPL process
- Load Unit Address,The LOAD parameter - dddxxsn,The LOADxx member
- The UNIX support in z/OS
- Displaying OMVS processes
- USS z/OS packaging
- z/OS and USS comparative functions
- Terminal and workstation support
- Special TSO/E commands
- Controlling z/OS UNIX - BPXPRMxx parmlib member
- Displaying OMVS information
- ulimit - a (shell command)
- New ISPF panels
- The Shell
- USS functions
- Processes and fork()
- fork() and shared storage
- spawn() function
- Inter-Process Communications functions
- Memory mapped files
- Threads
- Daemon processes
- The UNIX file system
- The system files - /etc, /dev, /bin and others
- Display File systems
- Security classification
- Multilevel security
- Security labels
- Security levels
- Security categories
- Dominance and equivalence.
- Practical exercise on each student's exclusive z/OS system

Users & Groups

- UNIX user definition
- Users & Groups
- User & Group Profiles
- RACF User/Group profile extensions
- UNIX identity with USP
- RACF commands for Users
- RACF commands for Groups
- System Resource limits
- OMVS segment – additions
- The SEARCH command
- Security administration
- SURROGAT class
- Surrogate authority
- FIELD Level access checking
- Using the FIELD class
- Security for OMVS
- Practical exercise on each student's exclusive z/OS system

Superusers & UID/GID Management

- User definition – superuser
- BPX.SUPERUSER
- Switch to superuser mode
- Superuser granularity
- UNIPRIV resource names
- UNIPRIV class

BMC Mainframe: RACF Security in a UNIX System Services Environment

COURSE ABSTRACT

- Managing UIDs
- Prevention of shared UIDs
- Shared UIDs
- Search enhancement to map UID & GID
- Automatic UID/GID assignment: The Started Task Table
- Using ICHRIN03
- Using the STARTED class
- Trusted and Privileged
- Practical exercise on each student's exclusive z/OS system

Application Identity Mapping

- Application Identity Mapping

z/OS UNIX File and Function Security

- Directories & files
- UNIX file security
- Protecting directories & files
- Access levels
- The File Security Packet (FSP)
- Reading File Permissions
- Basic - file authorisation checking
- File Permission – examples
- Protecting files
- chmod command examples
- chown command - change file owner
- chmod - change file mode (permissions)
- Protecting files
- File authorisation checking with UNIXPRIV
- RESTRICTED attribute
- Default file permissions & umask
- List file & directory information
- Interpreting ICH4081 messages
- Interpreting BPX messages
- Interpreting other messages
- Facility Class, FACILITY class profiles, FSACCESS class, FSEXEC class
- Practical exercise on each student's exclusive z/OS system

REXX Built-in Functions

- Introduction to REXX supplied built in functions
- How to use the most useful ones: ARG, DATE, TIME, DATATYPE, LENGTH, POS, WORDS, LEFT, RIGHT, STRIP, SPACE, COPIES and WORD
- This segment explains the commonly used REXX built-in functions, and indicates their use in REXX programs

Access Control Lists (ACLs)

- Access Control Lists (ACLs)
- Three Types of ACL
- Two types of Access ACL - base
- Two types of Access ACL – extended
- Permission Bits & ACLs
- Authority to create ACLs
- The getfacl & setfacl commands
- Getfacl
- Setfacl
- Managing ACLs
- getfacl - no ACLs
- getfacl - display ACLs for directory
- ACL examples
- setfacl - change permission bits
- ACL inheritance
- Directory default ACLs
- File default ACLs
- getfacl - display all ACLs
- UNIXPRIV & ACLs
- Authorisation checking – summary
- Recommendations
- Practical exercise on each student's exclusive z/OS system

Security for Daemons & Servers

- UNIX level security for daemons
- RACF profiles for daemon security
- Server overview
- UNIX level security for servers
- RACF profiles for server security
- Recommendations
- Maintaining a clean program environment
- Program profiles and libraries
- File extended attributes and authorities
- Protecting with BPX profiles
- Practical exercise on each student's exclusive z/OS system

Auditing UNIX System Services Security Events

- What can be audited
- New RACF classes
- RACF commands to implement
- SMF records
- UNIX commands to audit file access
- File Security Packet (FSP)
- UNIX commands to implement auditing
- List file & directory information
- Setting the auditing option in the FSP
- Auditing the superuser
- FSP reporting - HFS Unload
- Health Checkers
- Practical exercise on each student's exclusive z/OS system