COURSE ABSTRACT

BMC Mainframe: TCP/IP Security in a z/OS Environment using Policy Agent & RACF

COURSE CODE

» MGRS-TSZP-2021

APPLICABLE VERSIONS

» Not Applicable

DELIVERY METHOD

» Instructor-led Training (ILT)

COURSE DURATION

» 5 Days

PREREQUISITES

» BMC Mainframe: z/OS Communications Server Part 2 - Implementing TCP/IP under z/OS

» BMC Mainframe: RACF Security in a UNIX System Services Environment

RECOMMENDED TRAININGS

» NA

Course Overview

The course is developed and delivered by © RSM Technology.

Large system network security requirements have become much more stringent and complex over recent years, following the advent of TCP/IP and Internet interfaces. This essential new course explains how to set up and administer vitally important security for the z/OS networking environment.

The course gives attendees a sound understanding of how the Communications Server, along with other elements in z/OS including RACF, Policy Agent (PAGENT), z/OSMF and the Network Configuration Assistant, provide multiple IP security functions. These protect data privacy and integrity for z/OS and protect system resources from unauthorized access.

This course includes extensive hands-on exercises, with each student being given their own z/OS system on which to work.

Target Audience

All technicians responsible for setting up security in a TCP/IP for z/OS environment.

Learner Objectives

» Understand how RACF works

» Explain how z/OS SAF, especially RACF, is used to protect your network and communications

» Discuss the RACF Security profiles required to protect access to various network resources

» Understand how cryptography, Ciphers and SSL/TSL work in a z/OS environment

» Explain how to implement the TLS and SSL protocol technology to protect data exchanges between client and server applications

» Implement the SSH daemon and SFTP

» Describe how digital certificates can be implemented and used within z/OS and how various clients and servers use the certificates

» Implement Native TN3270/TLS security and Native FTPS/TLS security

» Explain how Digital Certificates are used in a policy-based z/OS environment

» Explain the rules and policies used in the Policy Agent (PAGENT) to dictate how users, applications and organizations access and use their IT resources

» Understand how the PAGENT can be configured as a Central Policy Server

» Understand how to use z/OSMF and Network Configuration Assistant

» Implement TN3270/Telnet security and FTPS using AT-TLS

» Explain how other applications use AT/TLS with PAGENT implement IP Security

» Implement TRMD and IKED

» Permit or deny IP packets into and out of z/OS using IP Filtering

» Describe at a high level how the IPSec tunnel traverses a NAT or NAPT device

» Implement IDS

» Implement DMD

» Describe the QoS concepts and how to implement QoS.

BMC Mainframe: TCP/IP Security in a z/OS Environment using Policy Agent & RACF

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

Understanding RACF Network Security

- Why secure the TCP/IP network
- What is required of a security system?
- IBM's Resource Access Control Facility (RACF)
- Main RACF - z/OS components
- How does RACF work?
- RACF profiles: Group profiles, User profiles, Dataset profiles, General resource profiles
- Resource classes
- RACF commands

RACF Group Structure

- RACF group structure
- RACF group types
- RACF group structure
- Dataset profile ownership
- Concept of profile ownership
- RACF administration delegation
- Benefits of RACF groups
- Defining RACF groups
- Group CONNECT authority
- Group profile segments
- Group related commands

Defining Users to RACF

- Information on users
- RACF user information
- Segment information: TSO segment information, NetView segment information, CICS segment information, OMVS segment information
- Defining a new user
- User- related commands
- User attributes
- Classifying users and data
- Security categories and levels
- Creating a Security Category
- Creating a Security Level
- How Security Categories and Levels are used
- Security labels

Dataset Profiles

- Dataset related commands
- Dataset protection: Discrete profiles, Generic profiles, Rules for defining dataset profiles
- Dataset profile ownership
- Defining generic profiles
- Access authority to datasets
- Adding dataset profiles – ADDSD
- PERMIT command
- Building access lists (PERMIT)

Defining General Resources

- General Resource related commands
- Class Descriptor Table (CDT)
- IBM-defined Resource Classes
- Steps for defining General Resource profiles
- Granting access to a General Resource
- Global Access Table (GAT)
- Setting up the Global Access Table (GAT)

Protecting Network Resources

- Tasks that need protection with SERVAUTH Class
- Policy based networking
- SERVAUTH Resource Class responsibilities
- SERVAUTH Resource Class
- Protecting the TCPIP stack
- Protecting your network access
- Application considerations when using NETACCESS
- Using the NETSTAT and PING commands to check protection

BMC Mainframe: TCP/IP Security in a z/OS Environment using Policy Agent & RACF

COURSE ABSTRACT

- Protecting your network ports
- RACF definitions for protecting network ports
- Using the NETSTAT command to check PORT access
- Protecting the use of socket options
- What are network commands
- Protecting network commands - z/OS TCPIP commands
- Protecting network commands - NETSTAT and ONESTAT commands
- Protecting network commands - EZACMD REXX program
- Protecting FTP access
- Other FTP profiles
- Protecting TN3270 Secure Telnet Port
- Protecting the MODDVIPA command

Cryptography, SSL, Ciphers & Digital Certificates

- overview
- What is a digital certificate?
- Public key & certificate
- Uses for certificates in applications
- Secure Sockets Layer (SSL)
- Secret key cryptography
- Ciphers used in secret key cryptography
- Notes on secret key ciphers
- Public key cryptography
- Public key ciphers
- Message integrity
- Message digest algorithms
- Message Authentication Codes
- Using the ciphers
- Ciphers
- SSL protocol
- How SSL works
- SSL Session ID
- The SSL layer
- System SSL
- System SSL on z/OS
- Why TLS
- Hardware cryptography on System Z
- Crypto support in z/OS
- SSL and Crypto devices
- Three types of encryption keys
- Clear Key processing
- Secure Key processing
- Master Keys and Key Data Sets
- Protected Key/Wrapping Key

SSHD and SFTP using SSL

- SSHD UNIX files
- SSHD - Using ICSF and /dev/random)
- SSHD - Creating configuration files
- SSHD - Creating SSHD server keys
- SSHD- Set up SSHD server userids
- SSHD - Create SSHD server started task
- SSHD - TCP configuration
- SSHD - Verify z/OS DNS / Resolver operation
- The FTP server
- FTPS and SFTP
- Pros and cons of FTPS and SFTP
- Customizing the FTP.DATA dataset
- Customizing the PROFILE & SERVICES datasets
- Starting FTP

RACF & Digital Certificates

- Cryptography in Internet applications
- Public key cryptography overview
- What is a digital certificate?
- Public key & certificate
- Uses for certificates in applications
- Secure Sockets Layer (SSL)
- Digital certificates and RACF
- How RACF uses digital certificates
- RACF classes & commands
- RACDCERT
- RACF certificate generation
- RACDCERT command
- Creating a certificate
- Gencert examples
- Key rings
- RACDCERT ring functions
- Certification installation
- RACDCERT ADD examples
- Certification installation
- Certificate management
- Exploiters of certificates
- Exporting a certificate
- Certificates are packaged in formats
- Steps for migrating a certificate and its ICSF private key in the PKDS
- KEYXFER Utility
- Miscellaneous issues
- Renew a certificate
- Examples of REKEY and ROLLOVER
- Certificate mapping
- RACF Key Rings
- Global FACILITYclass profiles
- Sharing a private key
- RDATALIB Class
- RACDCERT granular administration
- RACDCERT granular control
- Listing, removing & deleting
- Password enveloping
- How does password enveloping work?
- Password enveloping - exceptions

Secured TN3270 and FTPS

- What is TN3270 security?
- How native TN3270 security can be applied with TLS
- Description of TN3270 native connection security
- Dependencies for Telnet server native connection security
- Example of definitions
- Encryption algorithms (cipher suites)
- RACF permissions
- What is FTP security?
- Software and hardware prerequisites
- Configuring FTP native TLS security
- Logging onto the Server with FileZilla

Introduction to Policy Agent

- Introduction to policy based networking
- The Policy Agent

BMC Mainframe: TCP/IP Security in a z/OS Environment using Policy Agent & RACF

COURSE ABSTRACT

- RACF and PAGENT
- Define a User for PAGENT
- Give authorized users access to start and stop PAGENT
- Securing the pasearch command and initialising PAGENT before TCPIP
- Other address spaces that will need RACF profiles
- Central policy server
- SERVAUTH authorisation for Policy Client
- Basic configuration
- Defining the TcpImage statements
- Image definitions
- Logging
- PAGENT commands
- Traffic Regulation
- Management Daemon
- Policy infrastructure management services
- Implementation and operations
- Parameters for policy infrastructure management services

z/OSMF and Network Configuration Assistant

- z/OSMF and Network Configuration Assistant
- z/OSMF desktop and Network Configuration Assistant
- Backing store
- Creation of z/OS groups
- Creation of z/OS images and TCPIP stack
- TCPIP connectivity rules
- Creating your own Requirement Map
- Advanced Settings
- Advanced Settings – parameters
- Current backing store
- Installation of configuration files
- PAGENT requirements
- CSFSERV resource class
- Example for AT-TLS
- Example of Intrusion Detection Services
- Example of IP filtering
- Example of IP Security
- Example of Network Address Translation
- Example of IKE protocols
- Example of Quality of Service
- SNMP overview
- SNMP in operation

IP Security

- Setting up IPSec on z/OS
- Defining IPSec with Network Configuration Assistant
- IPSec Traffic Descriptors
- IPSec Security Levels
- IPSec Advanced Settings
- IPSec address groups
- IPSec Requirement Maps
- IPSec Reusable Rules
- Setting up IKED
- The IKED catalogued procedure and configuration file
- Reserve the ports and RACF changes
- Digital certificates for IKED
- Authorizing Callable Services
- Other actions for IPSec
- Commands for IPSec
- Using the IPSec policy in z/OS

Intrusion Detection Services & Defense Manager Daemon

- Basic concepts
- Scan policies
- There are different types of scan events
- Attack policies
- Attack policy notification
- Traffic regulation policies
- TCP traffic regulation
- UDP traffic regulation
- Implementing IDS
- Creating the IDS policy
- IDS traffic descriptors
- IDS Requirement Maps
- Creating a new IDS Requirement Map
- IDS scans
- Scan Levels
- Modify IDS scans
- IDS Traffic Regulation
- z/OSMF selection of requirement map
- Defensive filtering overview
- Simulate mode
- Installation of defensive filtering
- Filter types
- Defense Manager Daemon installation
- DMD Configuration File
- DMD started procedure
- Ipsec F command
- The Ipsec -t command