TCP/IP Security in a z/OS Environment using Policy Agent & RACF Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Overview

This course explains how to set up security for the z/OS networking environment. With the advent of TCP/IP and the Internet, network security requirements have become more stringent and complex. The Communications Server, along with other elements in z/OS including RACF and Policy Agent (PAGENT), provides IP security functions. These protect data privacy and intergrity for z/OS, and protect system resources from unauthorized access.
This is a 'workshop' style course, and attendees will work through extensive hands-on exercises, on their own z/OS system.

This course is also available 'on demand' (minimum 2 students) for additional public presentations or for one-company, on-site presentations.

Prerequisites

Attendees will need a sound knowledge of TCP/IP concepts and protocols (this can be gained by attending the RSM course **TCP/IP Fundamentals**), and TCP/IP in a z/OS environment (this can be gained by attending the RSM course **z/OS Communications Server Part 2 - Implementing TCP/IP under z/OS. A good knowledge of UNIX System Services is also needed, which can be gained by attending RSM's course Using RACF under UNIX System Services (USS).**

What You Will Learn

- 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
- describe how Digital Certificates can be implemented and used within z/OS and how various clients and servers use the certificates
- explain how Digital Certificates are used in a policy-based z/OS environment
- implement NSS using a daemon and a Client
- 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 configued as a Central Policy Server
- describe the QoS concepts and how to implement QoS
- permit or deny IP packets into and out of z/OS using IP Filtering
- explain how to implement IP Security
- describe at a high level how the IPSec tunnel traverses a NAT or NAPT device
- explain how to implement the TLS and SSL protocol technology to protect data exchanges between client and server applications
- implement TN3270/Telnet security and FTPS
- implement the SSH daemon and SFTP
- understand IDS
- configure policy based routing tables.

TCP/IP Security in a z/OS Environment using Policy Agent & RACF Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Outline

RACF Demystified

Protecting System Resources

Certificate Management in z/OS

Network Security Services

Policy Agent

Central Policy Server

Quality of Service

IP Filtering

IP Security

Network Address Translation Traversal Support

Application Transparent Transport Layer Security

SSH Daemon and SFTP

Intrusion Detection Services

Polcy Based Routing