Course Outline

CA Top Secret r15 for z/OS: Security Mainframe and Distributed Integrations 200

Course Summary

Description

CA Top Secret provides comprehensive security for the z/OS, z/VM and z/VSE environments—including z/OS UNIX and Linux for zSeries. Built-in, comprehensive administrative and reporting tools, along with detailed event logging capabilities, simplify the management of users and their access rights. This course will show you how to write CA Top Secret commands to configure the tools and generate reports.

Objectives

After taking this course, students will be able to:

- Create ACIDs and ADD/REMOVE attributes and ownership
- Define resources
- Allow limited access to resources
- Audit users and/or resources
- Query the security database
- Define authorities for alternate and/or decentralized administrators
- Generate CA Top Secret reports
- Describe basic control options and their functions

Topics

- CA Top Secret Overview
- Implementing Security Database Design
- Identifying Users to CA Top Secret
- Field Descriptor Table
- Static Data Table
- How to Protect Datasets and Volumes
- Determining the Search Algorithm
- Protecting Other Resources
- Resource Descriptor Table
- Defining Security Administration
- Defining Basic Global Control Options
- FACILITY Controls
- BATCH and STC FACILITYs
- Activating FACILITY
- Reports
- Recovery Procedures

Audience

- Security Administrators
- Security Managers
- Anyone taking an active part in security implementation or administration

Prerequisites

- Basic knowledge of mainframes
- Experience with OS/390 or VSE (or both)
- 3 months of working experience with CA Top Secret in your environment

Duration

Four Days

Course Outline

CA Top Secret r15 for z/OS: Security Mainframe and Distributed Integrations 200

Course Outline

I. *CA Top Secret Overview*
- A. Concepts underlying CA Top Secret
- B. Starting CA Top Secret and Security Validation
- C. How to LIST information associated with any ACID

II. *Implementing Security Database Design*
- A. Creating ZONE, DIVISION, and DEPARTMENT records
- B. Creating profile records for use with resource authorization
- C. Issuing commands to define databases
- D. Reporting on security file design

III. *Identifying Users to CA Top Secret*
- A. Creating user ACIDs
- B. Using attributes and privileges
- C. LIST ACID details

IV. *Field Descriptor Table*
- A. Using Field Descriptor table
- B. Defining Field Descriptor table entries

V. *Static Data Table*
- A. Calendar Records
- B. Time Records

VI. *How to Protect Datasets and Volumes*
- A. Defining datasets and volumes to the security file
- B. Authorizing datasets

VII. *Determining the Search Algorithm*
- A. Using the search algorithm
- B. Using search sequence in security administration
- C. Testing security file permissions with TSSIM

VIII. *Protecting Other Resources*
- A. Kinds of resources that can be protected
- B. Resource authorization, permission, and protection

IX. *Resource Descriptor Table*
- A. Using RDT
- B. Defining a new entry in RDT

X. *Defining Security Administration*
- A. Creating security administration ACIDs
- B. Decentralizing security admission

XI. *Defining Basic Global Control Options*
- A. Basic control options overview
- B. Listing and changing control options

XII. *FACILITY Controls*
- A. Predefined FACILITYs
- B. Using FACILITYs

XIII. *BATCH and STC FACILITYs*
- A. Activating BATCH FACILITY
- B. Activating STC FACILITY
- C. Defining a started task to the STC table

XIV. *Activating FACILITY*
- A. Creating a region ACID
- B. Defining a FACILITY

XV. *Reports*
- A. Using the utilities available

XVI. *Recovery Procedures*
- A. Fixing a primary security file
- B. Back and recovery
- C. Recovery procedures