A Broadcom Company

technologies

CA Top Secret® V16: Security Mainframe and Distributed Integrations 200

EDUCATION COURSE DESCRIPTION

SUPPORTED PRODUCT RELEASE(S)

CA Top Secret®
Version 16

COURSE TYPE, LENGTH, & CODE

- Instructor-Led Training (ILT)
- Four (4) Days
- Course Code: 06TSS20071

PREREQUISITE(S)

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

WHO SHOULD ATTEND

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

Course Overview

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.

This Course Will Show You How To:

- Describe features, components, and functions of CA Top Secret.
- 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

Course Agenda

Module 1: –CA Top Secret Overview

- Concepts underlying CA Top Secret
- Starting CA Top Secret and Security Validation
- Accessor ID (ACID) types and characteristics
- How to LIST information associated with any ACID

Module 2: Implementing Security Database Design

- Creating ZONE, DIVISION, and DEPARTMENT records
- Creating profile records for use with resource authorization
- Issuing commands to define databases
- Reporting on security file design

Module 3: Identifying Users to CA Top Secret

- Creating user ACIDs
- Using attributes and privileges
- Create profile ACIDs with FACILITY access
- LIST ACID details

Module 4: Field Descriptor Table

- Using Field Descriptor table
- Defining Field Descriptor table entries

Module 5: Static Data Table

- Use the SDT record
- Calendar Records
- Time Records

Module 6: How to Protect Datasets and Volumes

- Defining datasets and volumes to the security file
- Authorizing datasets
- Secure DASD/Tape volumes
- Use masking for resource authorization

Module 7: Determining the Search Algorithm

- Using the search algorithm
- Using search sequence in security administration
- Testing security file permissions with TSSIM

Module 8: Protecting Other Resources

- Kinds of resources that can be protected
- Protect other resources beyond datasets and volumes

Course Agenda Continued

Module 9: Resource Descriptor Table

- Using RDT
- Defining a new entry in RDT

Module 10: Defining Security Administrators

- Creating security administration ACIDs
- Decentralizing security admission

Module 11: – Defining Basic Global Control Options

- Basic control options overview
- Listing and changing control options

Module 12: FACILITY Controls

- Predefined FACILITYs
- Using FACILITYs

Module 13: BATCH and STC FACILITYs

- Activating BATCH FACILITY
- Activating STC FACILITY
- Defining a started task to the STC table

Module 14: Activating a FACILITY from Beginning to End

- Creating a region ACID
- Defining a FACILITY

Module 15: Reports

- Using the utilities available
- Set necessary parameters to run these utilities
- CA data-centric security and compliance solutions

Module 16: Recovery Procedures

- Fixing a primary security file
- Back and recovery
- Recovery procedures

Course Resources

Communities

CA Top Secret Community

Documentation

CA TOP SECRET® FOR Z/OS 16.0

Product Information

https://www.broadcom.com/products/mainframe/security-compliance/top-secret