ProTech Professional Technical Services, Inc.

CA ACF2 for z/OS Version 16.x: Foundations 200
Course Summary

Description

CA ACF2 for z/OS provides innovative and comprehensive security for various business transaction environments that enable you to fully realize the reliability, scalability, and cost effectiveness of the mainframe.

This course will show you how CA ACF2 provides protection by default. You will also learn about control databases and how to write, compile, decompile, and test CA ACF2 access rules for data sets

Objectives

After taking this course, students will be able to:

- Understand how general IT security goals and procedures apply to the mainframe and how they increase security administration productivity.
- Understand how CA ACF2 is organized, its capabilities, and design philosophy.
- Create and maintain LOGONID (LID) records, which identify each user on a system protected by CA ACF2.
- Understand the function and structure of the LID record, which is key to security administrators and account managers effectively leveraging their own privileges and managing the users within their scope.
- Secure critical data and assets by understanding how CA ACF2 processes dataset access rules.
- Secure resources to control system configuration and the processes necessary for system integrity.

Topics

- Mainframe Security Overview
- Features and Capabilities
- LOGONID Concepts
- Work with Log on IDs
- Secure Data
- Resource Rules
- Secure Resources

Audience

This course is designed for:
- Security and System Administrators
- Information Assurance Staff
- IT Auditors
- Data Owners

Prerequisites

- Basic understanding of Information Technology concepts and terminology
- Basic TSO/ISPF operational experience

Duration

Four or Five Days

Course Outline (vertical, left margin)

CA ACF2 for z/OS Version 16.x: Foundations 200

Course Outline

I. *Mainframe Security Overview*
   A. Goals & Concepts
   B. Security Features
   C. Attack Vectors

II. *Features and Capabilities*
   A. Design Philosophy
   B. Control Databases
   C. Operating Environment

III. *LOGONID Concepts*
   A. LID Records & UID Strings
   B. Role-Based Access Control
   C. Display LID Records

IV. *Work with Log on IDs*
   A. Special User LIDs, Scope Security, & Account Privileges
   B. Create & Modify LID Records
   C. Activity Logs

V. *Secure Data*
   A. Access Rule Set Components, Rule Masking & Rule Processing
   B. CA ACF2 Subcommands
   C. Data Set Violation Reports

VI. *Resource Rules*
   A. Resource Rule Sets
   B. Rule Set Elements
   C. Rule Masking

VII. *Secure Resources*
   A. System Resources
   B. Maintain Resource Rules
   C. Identify Reports