Course Outline

CA ACF2 r12 Advanced Administration 400

Course Summary

Description

This course will teach you how to use CA ACF2 Security to identify and control access to sensitive data, including z/OS operating system files. You will gain hands-on experience with system entry validation for online, batch jobs and started task control (STC) Logon IDs. In addition, you will be taught how to configure Global System Options (GSO) and discuss their effects on global users and the system. You will also be taught other advanced techniques and concepts, such as redefining a more effective user identification (UID) string, employing decentralized security administration techniques, solving bypass label processing exposures, setting PDS member level security, and defining a MUSASS system and reporting options.

Objectives

By the end of this course, students will be able to:

- Identify and protect sensitive data, such as payroll and billing, and most important, the critical data of the z/OS operating system files and data sets
- Identify and maintain Global System Options (GSO)
- Implement and use the System Authorization Facility (SAF)
- Customize CA ACF2 for your unique business environment
- Describe the processing involved with online, batch jobs and started tasks
- Identify and implement advanced techniques for multiple functions including Nextkey, Decentralized Security Administration, User Defined InfoStorage Records and Command Propagation
- Recover data after a disaster
- Define and set up CICS and other multiuser address spaces

Topics

- Basic Review
- Critical File Identification and Protection
- Global System Options (GSO)
- System Authorization Facility (SAF)
- Administrative Fine Tuning
- Define CICS and Other Multiuser Address Spaces
- Command Propagation Facility (CPF)
- Reporting Options

Audience

This course is designed for:

- Security Administrators
- Systems Programmers
- Security Auditors

Prerequisite

- CA ACF2 r12: Basic Administration 200 (06ACF20031)
- CA ACF2 r12: Intermediate Administration 300 (06ACF30191)

Duration

Three Days

Course Outline

CA ACF2 r12 Advanced Administration 400

Course Outline

I. Basic Review
A. Basic Security Concepts and Review
B. Control Databases
C. VSAM Key to the Record
D. User Identification (UID) String, Rules, System Options

II. Critical File Identification and Protection
A. Protecting z/OS System Files
B. System Entry Validation
C. Advanced Program Path
D. Disaster Recovery

III. Global System Options (GSO)
A. Purpose of GSO Records
B. Major GSO Records
C. GSO Password Record
D. GSO Options Record
E. GSO Levels of Protection
F. Commands That Maintain GSO Records

IV. System Authorization Facility (SAF)
A. GSO SAFDEF Records
B. GSO CLASMAP Records
C. SECTRACE

V. Administrative Fine Tuning
A. Redefine the UID String
B. Decentralized Security Administration
C. Effective Nextkeys
D. Controlling Bypass Label Processing (BLP)
E. PDS Member Level Protection
F. User-Defined Infostorage Records

VI. Define CICS and Other Multiuser Address Spaces
A. MUSASS Logon ID Record
B. MUSASS GSO Definitions
C. MUSASS Control Records

VII. Command Propagation Facility (CPF)
A. CPF Requirements
B. CPF Processing Flow
C. CPF Control Records

VIII. Reporting Options
A. JCL Used in Batch JOB
B. Standard Reports
C. CAEarl Reports