Course Outline

# CA ACF2 for z/OS Version 16.x: Intermediate Administration 300

## Course Summary

### Description

The success of today's business strategies depends on a reliable and cost-effective security infrastructure. Businesses need web access to their mainframe databases, but without the stress of security concerns. Consumers want their online personal information to be protected. CA ACF2 for z/OS (CA ACF2) provides comprehensive security for your valuable information assets, enabling your business to fully realize the reliability, scalability and cost-effectiveness of the mainframe.

This course focuses on the features of CA ACF2 that provide default protection for your mainframe operating systems. The material covered in this course will be reinforced through case studies and hands-on lab exercises.

This course contains the same information as the Web-Based Training courses offered separately (06ACF30230, 06ACF30240, 06ACF30250, 06ACF30260, 06ACF30270, 06ACF30280, 06ACF30290, 06ACF30300, 06ACF30310, 06ACF30320, 06ACF30330, and 06ACF30340).

### Objectives

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

- Describe the basic GSO record types and their maintenance procedures
- Extend and apply limits to CA ACF2 privileges in a dynamic and granular fashion
- Leverage profile records to retain additional information about users and z/OS resources
- Apply cross-reference records to organize diversely named resources, users, and sources into application-oriented group entities
- Describe verification and security policy across the entire enterprise using digital certificates
- Apply verification and security policy across the entire enterprise using digital certificates
- Describe PDS member-level protection

### Topics

- Describe Basic GSO Options
- Apply Privilege Control
- Leverage Profile Records
- Apply Cross Reference Records
- Describe Digital Certificates
- Apply Digital Certificates
- Secure FTP
- Secure USS
- Secure MQ
- Secure CICS
- Secure IMS
- PDS Member Level Protection

### Audience

This course is designed for:

- Security Administrators
- System Administrators
- Information Assurance Staff
- IT Auditors
- Data Owners

Course Outline

# CA ACF2 for z/OS Version 16.x: Intermediate Administration 300

## Course Summary (cont.))

### Prerequisite

- Basic understanding of Information
- Technology concepts and terminology
- Basic TSO/ISPF operational experience
- CA ACF2 for z/OS Version 16.x: Foundations 200 06ACF20091

### Duration

Two Days

Course Outline

# CA ACF2 for z/OS Version 16.x: Intermediate Administration 300

## Course Outline

### I. Describe Basic GSO Options
A. Describe the basic GSO record types and APPLDEF records
B. Describe the GSO EXITS record fields
C. Describe the GSO OPTS record fields
D. Utilize GSO wildcard searches and sorts

### II. Apply Privilege Control
A. Extend and apply limits to CA ACF2 privileges in a dynamic and granular fashion
B. Provide a stronger implementation to meet corporate security goals
C. Defining special privileges and controls

### III. Leverage Profile Records
A. Leverage profile records to retain additional information about users and z/OS resources
B. Identify Profile Administration commands
C. Describe Profile record structure
D. Identify Profile record segments

### IV. Apply Cross Reference Records
A. Identify cross-reference record types
B. Describe cross-reference record structure features
C. Identify Source, Resource, and Role groups
D. Identify Roles

### V. Describe Digital Certificates
A. Describe verification and security policies using digital certificates
B. Describe digital certificates
C. Process digital certificate with CA ACF2
D. Identify digital certificate tools, support, and commands.

### VI. Apply Digital Certificates
A. Apply verification and security policies across the entire enterprise using digital certificates
B. Describe the CERTDATA and KEYRING User Profile records
C. Associate a certificate with a LID

### VII. Secure FTP
A. Use Mainframe FTP
B. Describe setup requirements
C. Apply configuration

### VIII. Secure USS
A. Secure USS to enable programs running under USS to have full, secure access to the other internal functions of z/OS

### IX. Secure MQ
A. Describe the basic GSO record types and APPLDEF records
B. Describe the GSO EXITS record fields
C. Describe the GSO OPTS record fields
D. Utilize GSO wildcard searches and sorts

### X. Secure CICS
A. Extend and apply limits to CA ACF2 privileges in a dynamic and granular fashion
B. Provide a stronger implementation to meet corporate security goals
C. Defining special privileges and controls

### XI. Secure IMS
A. Leverage profile records to retain additional information about users and z/OS resources
B. Identify Profile Administration commands
C. Describe Profile record structure
D. Identify Profile record segments

### XII. PDS Member Level Protection
A. Describe PDS member-level protection
B. Implementation of PDS member-level protection