

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



Course Overview

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 the control databases and how they can be used to write, compile, decompile, and test CA ACF2 Access Rules for data sets.

This course is broken into multiple parts. Each part can be taken individually, or as part of the complete course. If all modules are taken, it is recommended that they be taken in the order listed on page 2 of this course description.

PRODUCT RELEASE

CA ACF2 for z/OS Version 16.x

COURSE TYPE, LENGTH & CODE

- WBT

Length

- Part 1: 15 minutes
- Part 2: 30 minutes

Code

- Part 1: 06ACF20100
- Part 2: 06ACF20110

PREREQUISITES

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

WHO SHOULD ATTEND

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

What You Will Learn

At the end of this course you will:

- Understand how general IT Security goals & procedures apply to the mainframe and how they increase security administration productivity
- Understand how ACF2 is organized, its' capabilities and design philosophy

For Managers

In this course, your employees will learn how CA ACF2 provides protection by default. They will also learn about the control databases and how they can be used to write, compile, decompile, and test CA ACF2 Access Rules for data sets.

This course is broken into multiple parts. Each part can be taken individually, or as part of the complete course. If all modules are taken, it is recommended that they be taken in the order listed on page 2 of this course description.

LEARNING PATH

<https://learningpaths.ca.com/acf2>

Course Agenda

Part 1: Mainframe Security Overview

- Describe basic IT security goals and concepts
- Identify innate MVS security features
- Identify potential MVS attack vectors

Part 2: Features and Capabilities

- Describe the CA ACF2 design philosophy
- Describe the CA ACF2 control databases
- Describe the CA ACF2 operating environment



Visit www.ca.com/education to explore the many course offerings, training options, and education solutions available to meet your skill development needs, budget, and travel requirements.