CA EDUCATION COURSE DESCRIPTION

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

SUPPORTED PRODUCT RELEASE(S)

CA ACF2 for z/OS
Version 16.x

COURSE TYPE, LENGTH, & CODE

Web-Based Training (WBT) with simulations

- Mainframe Security Overview: 06ACF20100 – 15 minutes
- Features and Capabilities: 06ACF20110 – 30 minutes
- Logonid Concepts: 06ACF20120 – 45 minutes
- Work with Logonids: 06ACF20130 – 1 hour, 30 minutes
- Secure Data: 06ACF20140 – 1 hour, 15 minutes
- Resource Rules: 06ACF20150 – 1 hour, 30 minutes
- Secure Resources: 06ACF20160 – 1 hour

PREREQUISITE(S)

- 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

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. This course contains the same information as the Instructor-Led Training (06ACF20091).

This Course Will Show You How To:

- Explain how general IT Security goals and procedures apply to the mainframe and how they increase security administration productivity
- Identify how 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.
- Identify 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.

Course Agenda

Mainframe Security Overview (06ACF20100):

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

Features and Capabilities (06ACF20110):

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

Logonid Concepts (06ACF20120):

- Describe LID recordings and UID strings
- Describe role-based access control
- Display LID records using CA ACF commands

Work with Logonids (06ACF20130):

- Describe special user LIDs, scope security, and account privileges
- Create and modify LID records
- Examine activity logs

Secure Data (06ACF20140):

- Describe access rule set components, rule masking capabilities, and rule processing
- Maintain rules using CA ACF2 subcommands
- Identify data set violation reports

Resource Rules (06ACF20150):

- Describe CA ACF2 resource rule sets
- Describe the elements of the resource rule set
- Describe rule masking capabilities

Secure Resources (06ACF20160):

- Protect and define various system resources
- Maintain resource rules using CA ACF2 commands
- Identify CA ACF2 resource rule related reports

Copyright © 2018 CA. All rights reserved. CA confidential and proprietary information for CA internal use only. No unauthorized copying or distribution permitted.

Course Resources

Communities

https://communities.ca.com/community/ca-mainframe-security

Learning Path

https://learningpaths.ca.com/acf2

Documentation

https://docops.ca.com/ca-acf2-for-z-os/16-0/en

Product Information

https://www.ca.com/us/products/ca-acf2.html

Copyright © 2018 CA. All rights reserved. CA confidential and proprietary information for CA internal use only. No unauthorized copying or distribution permitted.