ABSTRACT

BMC AMI CLOUD

BMC AMI Cloud 4: Customizing and Configuring (Workshop)

Learning Path >

Course Code: ACAC-CUCO-F403-W

Modality	Duration	Applicable Versions	Target Audience
Workshop	0.5 Day	4.2, 4.3	• Administrators • SysProg

Course Overview

BMC AMI Cloud is a suite of products built on a scalable, secure, and robust platform that you can use to accelerate your data-led journey to the cloud.

The BMC AMI Cloud Data platform consolidates the functionality of multiple storage, backup, and tape management products into a single, software-defined secondary data management solution, eliminating the need for physical and virtual tape libraries.

BMC AMI Cloud 4: Customizing and Configuring is a hands-on course that teaches how to prepare, operate, and secure a BMC AMI Cloud environment after installation. By the end of the course, participants can manage a stable, secure, and compliant AMI Cloud deployment suitable for long-term production use.

Prerequisites

- BMC AMI Cloud 4: Agent Installation (Workshop)
- BMC AMI Cloud 4: CDS Installation (Workshop)
- BMC AMI Cloud 4: Management Server Installation (Workshop)

Recommended Trainings

- BMC AMI Cloud 4: Fundamentals Using and Administering Concepts (Workshop)
- BMC AMI Cloud 4: Fundamentals Installing and Configuring Concepts (Workshop)

Learning Objectives

- Determine or validate production readiness, object storage selection, network validation, workload management, backup strategies, lifecycle management, and operational monitoring.
- Secure the environment through TLS, certificates, and trust management with RACF, access control best practices, and secure communication between components.
- Configure and validate import policies for DFSMSrmm users and understand how those policies interact with retention, WORM, and storage rules.

Course Modules

Module 1: Setup and Operations

- Validate a post-installation AMI Cloud environment using logs and configuration checks.
- Explain object storage concepts, including WORM, versioning, and retention policies.
- Select and configure an appropriate object storage solution for their environment.
- Secure object storage credentials using supported obfuscation methods.
- Verify network connectivity between the management server, worker, and object storage.
- Configure ISPF to use the correct ML2 default volume for archive processing.
- Assign an appropriate WLM service class to AMI Cloud components.
- Implement backup procedures for the management server and database.
- Schedule lifecycle management tasks to support retention and cleanup.
- Monitor policy execution and system health using SDSF and log output.

Module 2: Security and Trust Configuration

- Describe how TLS/SSL is used within BMC AMI Cloud architecture.
- Configure trust stores and keystores for the management server and worker components.
- Enable certificate verification for object storage connections.
- Import CA-signed and self-signed certificates into RACF.
- Create and manage RACF keyrings and SAF virtual keyrings.
- Identify and manage certificate expiration risks and renewal processes.
- Apply security best practices for AMI Cloud deployments.
- Implement role-based access control for administrators and operators.
- Configure and validate the BMC AMI Cloud Import policy for DFSMSrmm users.
- Align import policies with retention and storage rules to support compliance.