Implementing Microsoft Identity Manager (MIM) 2016

Course Duration: 32 Hours (4 Days)

Overview

The Implementing Microsoft Identity Manager (MIM) 2016 course is designed to provide IT professionals with the knowledge and skills needed to implement and manage Microsoft's Identity Manager solution. This Identity and Access management Training focuses on the MIM components and capabilities, including Identity synchronization, End-user self-service, and maintaining access management for users within an organization. Throughout the course, learners will delve into various modules, starting with an introduction to MIM (Module 1) and progressing through the intricacies of the Synchronization Service Manager (Module 2), Advanced synchronization methods (Module 3), and the management of Identity synchronization via MIM Service and Portal (Module 4). The course also covers synchronization management from the portal (Module 5), credential management (Module 6), group management (Module 7), and other essential considerations (Module 8).By the end of the course, participants in Identity and Access management Training India and worldwide will have a thorough understanding of how to implement, configure, and manage MIM to improve their organization's identity management systems.

Audience Profile

The Implementing Microsoft Identity Manager 2016 course is tailored for IT professionals specializing in identity management solutions.

- Systems Engineers responsible for managing identity infrastructure.
- Identity Managers overseeing user identity lifecycle.
- IT Administrators managing user accounts and access control.
- Security Administrators ensuring secure authentication and authorization.
- Infrastructure Architects developing identity management strategies.
- Consultants specializing in Microsoft identity technologies.
- Technical Support Staff handling identity management solutions.
- Compliance Officers ensuring adherence to access control and security policies.

Course Syllabus

Module 1: Introducing Microsoft Identity Manager

- This module provides an overview of the built-in features of Microsoft Identity Manager (MIM) through a user experience tour. Students will become familiar with the interface, high-level architecture, and the business needs MIM addresses. The module showcases the "finished product," setting the stage for subsequent modules where students will build the system from a raw installation. The lab includes creating a new user, managing groups and credentials for that user, and experiencing the new user's perspective.

Module 2: The Synchronization Service Manager

- This module introduces the MIM Synchronization Service Manager, explaining its features through scenarios that do not involve the MIM Portal. Key tools such as the Metaverse Designer, Operations

Tool, and Joiner are covered, along with basic configuration of a Management Agent (MA), run profiles, result verification, and simple Metaverse searches. In the lab, students will create a new MA for a basic HR system.

Module 3: More about Synchronization

- This module delves into various types of MAs, including LDAP and file-based sources, with an emphasis on inbound and outbound synchronization. Topics include filters, join and projection rules, connectors, disconnectors, provisioning, deprovisioning, and attribute flows. In the lab, students will create two additional MAs and establish a data-driven scenario for managing a directory (AD LDS).

Module 4: The MIM Service and Portal

- This module examines the MIM Service and application database, introducing key concepts like sets, workflows, policies, and permission management. Students will learn how the MIM Service integrates with the Synchronization Service and how data flows between them. In the labs, a MIM MA is built, allowing HR data to flow from the Synchronization Service to the portal and vice versa.

Module 5: Managing Synchronization from the Portal

- This module introduces portal-based Synchronization Rules, comparing them with “Classic” Rules. Students will explore the use of Portal Synchronization Rules, Workflows, and Management Policy Rules (MPRs), including complex attribute flows. Special considerations for managing Active Directory (AD) user accounts are also covered. The lab focuses on configuring MIM to automatically create (provision), rename, and remove (deprovision) AD user accounts as needed.

Module 6: Credential Management

- This module primarily focuses on password management, discussing topics such as self-service password reset (via text message, email, and MFA) and account unlocking (a new feature in MIM). Password synchronization is also covered. While advanced topics like custom password workflows and Azure MFA configuration are not addressed in depth, the labs cover nearly all key aspects of password management in MIM.

Module 7: Group Management

- This module addresses the management of distribution and security groups, including the relationship between groups in AD and other systems. Topics include Synchronization Rules, Workflows, MPRs, and configuring workflow approvals. The lab builds on the existing scenario to include the management of various group types in AD.

Module 8: Other Considerations

- This module consolidates key concepts of the MIM Service, focusing on MPRs (types, uses, processing, and troubleshooting). Operational considerations such as managing run cycles with scripts, backups, restores, and disaster recovery are also covered. Labs explore additional MPR features and operational matters. The final lab completes the proof-of-concept system. Additionally, this module provides an overview of Role-Based Access Control (RBAC) and Privileged Access Management as extensions of MIM’s capabilities.