SC-300T00-AC Microsoft Identity and Access Administrator

Overview

Course Duration: 4 Days

About This Course

The Microsoft Identity and Access Administrator course explores how to design, implement, and operate an organization's identity and access management systems by using Azure AD. Learn to manage tasks such as providing secure authentication and authorization access to enterprise applications. You will also learn to provide seamless experiences and self-service management capabilities for all users. Finally, learn to create adaptive access and governance of your identity and access management solutions ensuring you can troubleshoot, monitor, and report on your environment. The Identity and Access Administrator may be a single individual or a member of a larger team. Learn how this role collaborates with many other roles in the organization to drive strategic identity projects. The end goal is to provide you knowledge to modernize identity solutions, to implement hybrid identity solutions, and to implement identity governance.

Audience Profile

This course is for the Identity and Access Administrators who are planning to take the associated certification exam, or who are performing identity and access administration tasks in their day-to-day job. This course would also be helpful to an administrator or engineer that wants to specialize in providing identity solutions and access management systems for Azure-based solutions, playing an integral role in protecting an organization.

Course Outline

Module 1: Explore identity and Azure AD
Module 2: Implement initial configuration of Azure Active Directory
Module 3: Create, configure, and manage identities
Module 4: Implement and manage external identities
Module 5: Implement and manage hybrid identity
Module 6: Secure Azure Active Directory users with Multi-Factor Authentication
Module 7: Manage user authentication
Module 8: Plan, implement, and administer Conditional Access
Module 9: Manage Azure AD Identity Protection
Module 10: Implement access management for Azure resources
Module 11: Plan and design the integration of enterprise apps for SSO
Module 12: Implement and monitor the integration of enterprise apps for SSO
Module 13: Implement app registration
Module 14: Plan and implement entitlement management
Module 15: Plan, implement, and manage access review
Module 16: Plan and implement privileged access
Module 17: Monitor and maintain Azure Active Directory

Prerequisites

Before attending this course, students should have understood of:

- Security best practices and industry security requirements such as defense in depth, least privileged access, shared responsibility, and zero trust model.
- Be familiar with identity concepts such as authentication, authorization, and active directory.
- Have some experience deploying Azure workloads. This course does not cover the basics of Azure administration, instead the course content builds on that knowledge by adding security specific information.
- Some experience with Windows and Linux operating systems and scripting languages is helpful but not required. Course labs may use PowerShell and the CLI.