Microsoft Identity and Access Administrator (SC-300) Training

Duration: **4 Day**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Overview

The Microsoft Identity and Access Administrator course explores how to design, implement, and operate an organization's identity and access management systems by using Microsoft Entra ID. 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.

Prerequisites

Successful learners will have prior knowledge and understanding 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.
- Prerequisite courses (or equivalent knowledge and hands-on experience):
- MSC900 Microsoft Security, Compliance, and Identity Fundamentals

Important This course may require the use of Multifactor Authentication (MFA). Please read this page and download the Microsoft Authenticator app (or similar app) prior to attending the course

https://www.qa.com/resources/faqs/mfa-requirements/

Please see the below Microsoft article for further information on reasons for the MFA requirement:

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication

Target audience

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.

Microsoft Identity and Access Administrator (SC-300) Training

Duration: **4 Day**

BİLGİNÇ IT Academy
info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

What You Will Learn

- Build and configure a Microsoft Entra system.
- Implement and administer your access management using Microsoft Entra ID. Use MFA, Conditional Access, and identity protection to manager your identity solution
- How applications can and should be added to your identity and access solution with application registration in Microsoft Entra ID.
- Design and implement identity governance for your identity solution using entitlement, access reviews, privileged access, and monitoring your Microsoft Entra ID.

Outline

Learning path 1 - Implement an identity management solution

- Implement initial configuration of Microsoft Entra ID
- Create, configure, and manage identities
- Implement and manage external identities
- Implement and manage hybrid identity

Lab - Manage User Roles

Lab - Working with Tenant Properties

Lab - Assigning licenses using group membership

Lab - Configure external collaboration settings

Lab - Add guest users to the directory

Lab - Add a federated identity provider

Learning path 2 - Implement an Authentication and Access Management solution

- Secure Microsoft Entra users with multifactor authentication
- Manage user authentication
- Plan, implement, and administer Conditional Access
- Manage Microsoft Entra Identity Protection
- Implement access management for Azure resources
- Deploy and Configure Microsoft Entra Global Secure Access

Lab - Enable multi-factor authentication

Lab - Enable Microsoft Entra self service password reset

Lab - Microsoft Entra ID Authentication for Windows and Linux Virtual Machines

Lab - Assign Azure resource roles in Privileged Identity Management

Lab - Manage Microsoft Entra smart lockout values

Lab - Implement and test a conditional access policy

BİLGİNÇ IT Academy

info@bilginc.com
+44 20 3807 0925
+90 212 282 7700

Lab - Enable sign in and user risk policies

Lab - Configure an Multifactor authentication registration policy

Lab - Using Azure Key Vault for Managed Identities

Learning path 3 - Implement Access Management for Apps

- Plan and design the integration of enterprise apps for SSO
- Implement and monitor the integration of enterprise apps for SSO
- Implement app registration
- Register apps using Microsoft Entra ID

Lab - Defender for Cloud Apps application discovery and enforcing restrictions

Lab - Defender for Cloud Apps Access Policies

Lab - Register an application

Lab - Implement access management for apps

Lab - Grant tenant-wide admin consent to an application

Learning path 4 - Plan and implement an identity governance strategy

- Plan and implement entitlement management
- Plan, implement, and manage access review
- Plan and implement privileged access
- Monitor and maintain Microsoft Entra ID
- Explore the many features of Microsoft Entra Permissions Management

Lab - Create and manage a catalog of resources in Microsoft Entra entitlement management

Lab - Add terms of use and acceptance reporting

Lab - Manage the lifecycle of external users in Microsoft Entra Identity Governance settings

Lab - Creating Access Reviews for Internal and External Users

Lab - Configure Privileged Identity Management for Microsoft Entra roles

Lab - Microsoft Sentinel Kusto Queries for Microsoft Entra data sources

Lab - Monitor and managed security posture with Identity Secure Score