SC-300T00: Microsoft Identity and Access Administrator

Course Duration: 32 Hours (4 Days)

Overview

The SC-300T00: Microsoft Identity and Access Administrator course is designed to provide learners with comprehensive knowledge and expertise in managing, implementing, and monitoring an organization's identity and access management solutions using Microsoft Azure Active Directory (Azure AD). It is ideal for IT professionals who wish to enhance their skills in identity protection, governance, and ensuring secure access to applications within their corporate environment. Throughout the course, participants will dive into Configuring Azure AD, Managing various identities, Handling external and hybrid identities, and Securing authentication methods. They will gain skills in implementing Azure Multi-Factor Authentication (MFA), Conditional access policies, and managing User authentication. The course also covers the integration of apps for Single Sign-On (SSO), App registration processes, and establishing a robust Identity governance strategy, including Entitlement management, Access reviews, and Privileged access management. By mastering these areas, learners will be equipped to monitor and maintain Azure Active Directory effectively, ensuring a secure and compliant identity management framework within their organizations.

Audience Profile

The SC-300T00 course equips IT professionals with skills in Microsoft Identity and Access Management solutions, focusing on Azure Active Directory.

Target audience for the SC-300T00 course includes:

- System Administrators
- Network Administrators
- Identity and Access Administrators
- Azure Administrators
- IT Support Staff
- Security Engineers
- Compliance Officers
- Cloud Solution Architects specializing in security
- Enterprise Architects with a focus on identity and access management
- IT Professionals looking to gain knowledge in identity protection and access control within Azure environments

Course Syllabus

Module 1: Implement an identity management solution

Learn to create and manage your initial Azure Active Directory (Azure AD) implementation and configure the users, groups, and external identities you will use to run your solution.

Lessons

- Implement Initial configuration of Azure AD
- Create, configure, and manage identities
- Implement and manage external identities
- Implement and manage hybrid identity

After completing this module, students will be able to:

- Deploy an initial Azure AD with custom settings
- Manage both internal and external identities
- Implement a hybrid identity solution

Lab: Manage user roles

Lab: Setting tenant-wide properties

Lab: Assign licenses to users

Lab: Restore or remove deleted users

Lab: Add groups in Azure AD

Lab: Change group license assignments

Lab: Change user license assignments

Lab: Configure external collaboration

Lab: Add guest users to the directory

Lab: Explore dynamic groups

After completing this module, students will be able to:

- Deploy an initial Azure AD with custom settings
- Manage both internal and external identities
- Implement a hybrid identity solution

Module 2: Implement an authentication and access management solution

Implement and administer your access management using Azure AD. Use MFA, conditional access, and identity protection to manager your identity solution.

Lessons

- Secure Azure AD user with MFA
- Manage user authentication
- Plan, implement, and administer conditional access
- Manage Azure AD identity protection

Lab: Configure Azure AD MFA authentication registration policy

Lab: Enable sign-in risk policy

Lab: Manage Azure AD smart lockout values

Lab: Configure authentication session controls

Lab: Implement conditional access policies, roles, and assignments

Lab: Work with security defaults

Lab: Configure and deploy self-service password reset (SSPR)

Lab: Enable Azure AD MFA

After completing this module, students will be able to:

- Configure and manage user authentication including MFA
- Control access to resources using conditional access
- Use Azure AD Identity Protection to protect your organization

Module 3: Implement access management for Apps

Explore how applications can and should be added to your identity and access solution with application registration in Azure AD.

Lessons

- Plan and design the integration of enterprise for SSO
- Implement and monitor the integration of enterprise apps for SSO
- Implement app registration

Lab: Implement access management for apps

Lab: Create a custom role to management app registration

Lab: Register an application

Lab: Grant tenant-wide admin consent to an application

Lab: Add app roles to applications and recieve tokens

After completing this module, students will be able to:

- Register a new application to your Azure AD
- Plan and implement SSO for enterprise application
- Monitor and maintain enterprise applications

Module 4: Plan and implement an identity governance strategy

Design and implement identity governance for your identity solution using entitlement, access reviews, privileged access, and monitoring your Azure Active Directory (Azure AD).

Lessons

- Plan and implement entitlement management
- Plan, implement, and manage access reviews
- Plan and implement privileged access
- Monitor and maintain Azure AD

Lab: Configure PIM for Azure AD roles

Lab: Assign Azure AD role in PIM

Lab: Assign Azure resource roles in PIM

Lab: Connect data from Azure AD to Azure Sentinel

Lab: Create access reviews for groups and apps

Lab: Manage the lifecycle of external users with Azure AD identity governance

Lab: Add terms of use acceptance report

Lab: Create and manage a resource catalog with Azure AD entitlement

After completing this module, students will be able to:

- Manage and maintain Azure AD from creation to solution
- Use access reviews to maintain your Azure AD
- Grant access to users with entitlement management