SC-300T00: Microsoft Identity and Access Administrator

Days: 4

Description: This course provides IT Identity and Access Professional, along with IT Security Professional, with the knowledge and skills needed to implement identity management solutions based on Microsoft Azure AD, and it connected identity technologies. This course includes identity content for Azure AD, enterprise application registration, conditional access, identity governance, and other identity tools.

Prerequisites: Before attending this course, students should have an 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.

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.

Skills Gained:

- Implement an identity management solution
- Implement an authentication and access management solutions
- Implement access management for apps
- Plan and implement an identity governancy strategy

OUTLINE:

MODULE 1: IMPLEMENTING 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

LABS

- 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 user to the directory
- Lab: explore dynamic groups

SC-300T00: Microsoft Identity and Access Administrator

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

LABS

- 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

LABS

- 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 application and receive 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 GOVERNANCY 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

LABS

- 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 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