Training Course SC-300: Microsoft Identity and Access Administrator

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 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.

Duration: 4 Days.

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.

Certification: This course prepares you for the SC-300: Microsoft Identity and Access Administrator.

Course Objectives: After completing this course, students will be able to:

- Explore identity and Azure AD
- Implement initial configuration of Azure Active Directory
- Create, configure, and manage identities
- Implement and manage external identities
- Implement and manage hybrid identity
- Secure Azure Active Directory users with Multi-Factor Authentication
- Manage user authentication
- Plan, implement, and administer Conditional Access
- Manage Azure AD Identity Protection
- Implement access management for Azure resources
- Plan and design the integration of enterprise apps for SSO
- Implement and monitor the integration of enterprise apps for SSO
- Implement app registration

- Plan and implement entitlement management
- Plan, implement, and manage access review
- Plan and implement privileged access
- Monitor and maintain Azure Active Directory.

Course Outline:

1- Implement an identity management solution.
   - Define common identity terms and explain how they are used in the Microsoft Cloud.
   - Explore the common management tools and needs of an identity solution.
   - Review the goal of Zero Trust and how it is applied in the Microsoft Cloud.
   - Explore the available identity services in the Microsoft Cloud.

2- Implement initial configuration of Azure Active Directory
   - Implement initial configuration of Azure Active Directory.
   - Create, configure, and manage identities.
   - Implement and manage external identities (excluding B2C scenarios).
   - Implement and manage hybrid identity.

3- Create, configure, and manage identities.
   - Create, configure, and manage users.
   - Create, configure, and manage groups.
   - Manage licenses.
   - Explain custom security attributes and automatic user provisioning.

4- Implement and manage external identities.
   - Manage external collaboration settings in Azure Active Directory
   - Invite external users (individually or in bulk)
   - Manage external user accounts in Azure Active Directory
   - Configure identity providers (social and SAML/WS-fed)

5- Implement and manage hybrid identity.
   - Plan, design, and implement Azure Active Directory Connect (AADC)
   - Manage Azure Active Directory Connect (AADC)
   - Manage password hash synchronization (PHS)
   - Manage pass-through authentication (PTA)
   - Manage Seamless Single Sign-On (Seamless SSO)
   - Manage federation excluding manual ADFS deployments
   - Troubleshoot synchronization errors
   - Implement and manage Azure Active Directory Connect Health

6- Secure Azure Active Directory users with Multi-Factor Authentication
   - Learn about Azure AD Multi-Factor Authentication (Azure AD MFA)
   - Create a plan to deploy Azure AD MFA
   - Turn on Azure AD MFA for users and specific apps.

7- Manage user authentication.
   - Administer authentication methods (FIDO2 / Passwordless).
   - Implement an authentication solution based on Windows Hello for Business,
   - Configure and deploy self-service password reset.

- Deploy and manage password protection.
- Implement and manage tenant restrictions.

8- Plan, implement, and administer Conditional Access.
- Plan and implement security defaults.
- Plan conditional access policies.
- Implement conditional access policy controls and assignments (targeting, applications, and conditions).
- Test and troubleshoot conditional access policies.
- Implement application controls.
- Implement session management.
- Configure smart lockout thresholds.

9- Manage Azure AD Identity Protection.
- Implement and manage a user risk policy.
- Implement and manage sign-in risk policies.
- Implement and manage MFA registration policy.
- Monitor, investigate, and remediate elevated risky users.

10- Implement access management for Azure resources.
- Configure and use Azure roles within Azure AD.
- Configure and managed identity and assign it to Azure resources.
- Analyze the role permissions granted to or inherited by a user.
- Configure access to data in Azure Key Vault using RBAC-policy.

11- Plan and design the integration of enterprise apps for SSO.
- Discover apps by using MCAS or ADFS app report.
- Design and implement access management for apps.
- Design and implement app management roles.
- Configure pre-integrated (gallery) SaaS apps.

12- Implement and monitor the integration of enterprise apps for SSO.
- Implement token customizations.
- Implement and configure consent settings.
- Integrate on-premises apps by using Azure AD application proxy.
- Integrate custom SaaS apps for SSO.
- Implement application user provisioning.
- Monitor and audit access/Sign-On to Azure Active Directory integrated enterprise applications.

13- Implement app registration.
- Plan your line of business application registration strategy.
- Implement application registrations.
- Configure application permissions.
- Plan and configure multi-tier application permissions.

14- Plan and implement entitlement management.
- Define catalogs.
- Define access packages.
- Plan, implement and manage entitlements.
- Implement and manage terms of use.

- Manage the lifecycle of external users in Azure AD Identity Governance settings.

15- Plan, implement, and manage access review.

- Define a privileged access strategy for administrative users (resources, roles, approvals, and thresholds).
- Configure Privileged Identity Management for Azure AD roles.
- Configure Privileged Identity Management for Azure resources.
- Assign roles.
- Manage PIM requests.
- Analyze PIM audit history and reports.
- Create and manage emergency access accounts.

16- Plan and implement privileged access.

- Define a privileged access strategy for administrative users (resources, roles, approvals, and thresholds).
- Configure Privileged Identity Management for Azure AD roles.
- Configure Privileged Identity Management for Azure resources.
- Assign roles.
- Manage PIM requests.
- Analyze PIM audit history and reports.
- Create and manage emergency access accounts.

17- Monitor and maintain Azure Active Directory.

- Analyze and investigate sign in logs to troubleshoot access issues.
- Review and monitor Azure AD audit logs.
- Enable and integrate Azure AD diagnostic logs with Log Analytics / Azure Sentinel.
- Export sign in and audit logs to a third-party SIEM (security information and event management).
- Review Azure AD activity by using Log Analytics / Azure Sentinel, excluding KQL (Kusto Query Language) use.
- Analyze Azure Active Directory workbooks / reporting.
- Configure notifications.