Microsoft Identity and Access Administrator

Course: SC 300T00

Length: 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.

Prerequisites

Before attending this course, students should have 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 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.

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

Microsoft Identity and Access Administrator

Course: SC 300T00

Length: 4 Days

Course Outline

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

Lab:

- Manage user roles
- Setting tenant-wide properties
- Assign licenses to users
- Restore or remove deleted users
- Add groups in Azure AD
- Change group license assignments
- Change user license assignments
- Configure external collaboration
- Add guest users to the directory
- Explore dynamic groups

After completing this module, students will be able to:

- Deploy an initail 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:

- Enable Azure AD MFA
- Configure and deploy self-service password reset (SSPR)
- Work with security defaults
- Implement conditional access policies, roles, and assignments
- Configure authentication session controls
- Manage Azure AD smart lockout values
- Enable sign-in risk policy
- Configure Azure AD MFA authentication registration policy

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

Microsoft Identity and Access Administrator

Course: SC 300T00

Length: 4 Days

Lab :

- Implement access management for apps
- Create a custom role to management app registration
- Register an application
- Grant tenant-wide admin consent to an application
- Add app roles to applications 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

Lab :

- Creat and manage a resource catalog with Azure AD entitlement
- Add terms of use acceptance report
- Manage the lifecycle of external users with Azure AD identity governance
- Create access reviews for groups and apps
- Configure PIM for Azure AD roles
- Assign Azure AD role in PIM
- Assign Azure resource roles in PIM
- Connect data from Azure AD to Azure Sentinel

After completing this module, students will be able to:

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