Microsoft Identity and Access Administrator

Duration: 4 Days

Course Description:

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.

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.

Course Outline:

Explore identity in Microsoft Entra ID

- Introduction
- Explain the identity landscape
- Explore zero trust with identity
- Discuss identity as a control plane
- Explore why we have identity
- Define identity administration
- Contrast decentralized identity with central identity systems
- Discuss identity management solutions
- Explain Microsoft Entra Business to Business
- Compare Microsoft identity providers
- Define identity licensing
- Explore authentication
- Discuss authorization
- Explain auditing in identity

Implement initial configuration of Microsoft Entra ID

- Introduction
- Configure company brand
- Configure and manage Microsoft Entra roles
- Exercise manages users roles
- Configure delegation by using administrative units
- Analyze Microsoft Entra role permissions
- Configure and manage custom domains
- Configure tenant-wide setting
- Exercise - setting tenant-wide properties

Create, configure, and manage identities

- Introduction
- Create, configure, and manage users
- Exercise - assign licenses to users
- Exercise - restore or remove deleted users
- Create, configure, and manage groups
- Exercise - add groups in Microsoft Entra ID
- Configure and manage device registration
- Manage licenses
- Exercise - change group license assignments
- Exercise - change user license assignments
- Create custom security attributes
- Explore automatic user creation

Implement and manage external identities

- Introduction
- Describe guest access and Business to Business accounts
- Manage external collaboration
- Exercise - configure external collaboration
- Invite external users - individually and in bulk
- Exercise - add guest users to directory
- Exercise - invite guest users bulk
- Demo - manage guest users in Microsoft Entra ID
- Manage external user accounts in Microsoft Entra ID
- Manage external users in Microsoft 365 workloads
- Exercise - explore dynamic groups
- Implement and manage Microsoft Entra Verified ID
- Configure identity providers
- Implement cross-tenant access controls

Implement and manage hybrid identity

- Introduction
- Plan, design, and implement Microsoft Entra Connect
- Implement manage password hash synchronization (PHS)
- Implement manage pass-through authentication (PTA)
- Demo - Manage pass-through authentication and seamless single sign-on (SSO)
- Implement and manage federation
- Trouble-shoot synchronization errors
- Implement Microsoft Entra Connect Health
- Manage Microsoft Entra Health

Secure Microsoft Entra users with multifactor authentication

- Introduction
- What is Microsoft Entra multifactor authentication?
- Plan your multifactor authentication deployment
- Exercise - Enable Microsoft Entra multifactor authentication
- Configure multi-factor authentication methods

Manage user authentication

- Introduction
- Administer FIDO2 and passwordless authentication methods
- Explore Authenticator app and OATH tokens
- Implement an authentication solution based on Windows Hello for Business
- Exercise configure and deploy self-service password reset
- Deploy and manage password protection
- Configure smart lockout thresholds
- Exercise - Manage Microsoft Entra smart lockout values
- Implement Kerberos and certificate-based authentication in Microsoft Entra ID
- Configure Microsoft Entra user authentication for virtual machines

Plan, implement, and administer Conditional Access

- Introduction
- Plan security defaults
- Exercise - Work with security defaults
- Plan Conditional Access policies
- Implement Conditional Access policy controls and assignments
- Exercise - Implement Conditional Access policies roles and assignments
- Test and troubleshoot Conditional Access policies
- Implement application controls
- Implement session management
- Exercise - Configure authentication session controls
- Implement continuous access evaluation

Manage Microsoft Entra Identity Protection

- Introduction
- Review identity protection basics
- Implement and manage user risk policy
- Exercise enable sign-in risk policy
- Exercise configure Azure Active Directory multifactor authentication registration policy
- Monitor, investigate, and remediate elevated risky users
- Implement security for workload identities
- Explore Microsoft Defender for Identity

COURSE OUTLINE

Implement access management for Azure resources

- Introduction
- Azure roles
- Configure custom Azure roles
- Create and configure managed identities
- Access Azure resources with managed identities
- Analyze Azure role permissions
- Configure Azure Key Vault RBAC policies
- Retrieve objects from Azure Key Vault
- Explore Microsoft Entra Permissions Management

Plan and design the integration of enterprise apps for SSO

- Introduction
- Discover apps by using Microsoft Defender for Cloud Apps and Active Directory Federation Services app report
- Configure connectors to apps
- Exercise implement access management for apps
- Design and implement app management roles
- Exercise create a custom role to manage app registration
- Configure preintegrated gallery SaaS apps
- Implement and manage policies for OAuth apps

Implement and monitor the integration of enterprise apps for SSO

- Introduction
- Implement token customizations
- Implement and configure consent settings
- Integrate on-premises apps with Microsoft Entra application proxy
- Integrate custom SaaS apps for single sign-on
- Implement application-based user provisioning
- Monitor and audit access to Microsoft Entra integrated enterprise applications
- Create and manage application collections

Implement app registration

- Introduction
- Plan your line of business application registration strategy
- Implement application registration
- Register an application
- Configure permission for an application
- Grant tenant-wide admin consent to applications
- Implement application authorization
- Exercise add app roles to an application and receive tokens
- Manage and monitor application by using app governance

Plan and implement entitlement management

- Introduction
- Define access packages
- Exercise create and manage a resource catalog with Microsoft Entra entitlement management
- Configure entitlement management
- Exercise adds terms of use acceptance report
- Exercise manages the lifecycle of external users with Microsoft Entra identity governance
- Configure and manage connected organizations
- Review per-user entitlements

Plan, implement, and manage access review

- Introduction
- Plan for access reviews
- Create access reviews for groups and apps
- Create and configure access review programs
- Monitor access review findings
- Automate access review management tasks
- Configure recurring access reviews

Plan and implement privileged access

- Introduction
- Define a privileged access strategy for administrative users
- Configure Privileged Identity Management for Azure resources
- Exercise configure Privileged Identity Management for Microsoft Entra roles
- Exercise assign Microsoft Entra roles in Privileged Identity Management
- Exercise assign Azure resource roles in Privileged Identity Management
- Plan and configure Privileged Access Groups
- Analyze Privileged Identity Management audit history and reports
- Create and manage emergency access accounts

Monitor and maintain Microsoft Entra ID

- Introduction
- Analyze and investigate sign-in logs to troubleshoot access issues
- Review and monitor Microsoft Entra audit logs
- Exercise connect data from Microsoft Entra ID to Microsoft Sentinel
- Export logs to third-party security information and event management system
- Analyze Microsoft Entra workbooks and reporting
- Monitor security posture with Identity Secure Score