SC-300: Microsoft Identity and Access Administrator

Course Outline

Note

The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. Related topics may be covered in the exam

Skills at a glance

- Implement and manage user identities (20–25%)
- Implement authentication and access management (25–30%)
- Plan and implement workload identities (20–25%)
- Plan and automate identity governance (20–25%)

Implement and manage user identities (20–25%)

Configure and manage a Microsoft Entra tenant

- Configure and manage built-in and custom Microsoft Entra roles
- Recommend when to use administrative units
- Configure and manage administrative units
- Evaluate effective permissions for Microsoft Entra roles
- Configure and manage domains in Microsoft Entra ID and Microsoft 365
- Configure Company branding settings
- Configure tenant properties, user settings, group settings, and device settings

Create, configure, and manage Microsoft Entra identities

- Create, configure, and manage users
- Create, configure, and manage groups

- Manage custom security attributes
- Automate bulk operations by using the Microsoft Entra admin center and PowerShell
- Manage device join and device registration in Microsoft Entra ID
- Assign, modify, and report on licenses

Implement and manage identities for external users and tenants

- Manage External collaboration settings in Microsoft Entra ID
- Invite external users, individually or in bulk
- Manage external user accounts in Microsoft Entra ID
- Implement Cross-tenant access settings
- Implement and manage cross-tenant synchronization
- Configure external identity providers, including protocols such as SAML and WS-Fed

Implement and manage hybrid identity

- Implement and manage Microsoft Entra Connect Sync
- Implement and manage Microsoft Entra Cloud Sync
- Implement and manage password hash synchronization
- Implement and manage pass-through authentication
- Implement and manage seamless single sign-on (SSO)
- Migrate from AD FS to other authentication and authorization mechanisms
- Implement and manage Microsoft Entra Connect Health

Implement authentication and access management (25–30%)

Plan, implement, and manage Microsoft Entra user authentication

- Plan for authentication

- Implement and manage authentication methods, including certificate-based, temporary access pass, OAUTH tokens, Microsoft Authenticator, and passkey (FIDO2)
- Implement and manage tenant-wide Multi-factor Authentication (MFA) settings
- Configure and deploy self-service password reset (SSPR)
- Implement and manage Windows Hello for Business
- Disable accounts and revoke user sessions
- Implement and manage Microsoft Entra password protection
- Enable Microsoft Entra Kerberos authentication for hybrid identities

Plan, implement, and manage Microsoft Entra Conditional Access

- Plan Conditional Access policies
- Implement Conditional Access policy assignments
- Implement Conditional Access policy controls
- Test and troubleshoot Conditional Access policies
- Implement session management
- Implement device-enforced restrictions
- Implement continuous access evaluation
- Configure authentication context
- Implement protected actions
- Create a Conditional Access policy from a template

Manage risk by using Microsoft Entra ID Protection

- Implement and manage user risk by using Identity Protection or Conditional Access policies

- Implement and manage sign-in risk by using Identity Protection or Conditional Access policies
- Implement and manage Multifactor authentication registration policies
- Monitor, investigate and remediate risky users and risky sign-ins
- Monitor, investigate, and remediate risky workload identities

Implement access management for Azure resources by using Azure roles

- Create custom Azure roles, including both control plane and data plane permissions
- Assign built-in and custom Azure roles
- Evaluate effective permissions for a set of Azure roles
- Assign Azure roles to enable Microsoft Entra ID login to Azure virtual machines
- Configure Azure Key Vault role-based access control (RBAC) and access policies

Implement Global Secure Access

- Deploy Global Secure Access clients
- Deploy Private Access
- Deploy Internet Access
- Deploy Internet Access for Microsoft 365

Plan and implement workload identities (20–25%)

Plan and implement identities for applications and Azure workloads

- Select appropriate identities for applications and Azure workloads, including managed identities, service principals, user accounts, and managed service accounts
- Create managed identities

- Assign a managed identity to an Azure resource
- Use a managed identity assigned to an Azure resource to access other Azure resources

Plan, implement, and monitor the integration of enterprise applications

- Plan and implement settings for enterprise applications, including application-level and tenant-level settings
- Assign appropriate Microsoft Entra roles to users to manage enterprise applications
- Design and implement integration for on-premises apps by using Microsoft Entra Application Proxy
- Design and implement integration for software as a service (SaaS) apps
- Assign, classify, and manage users, groups, and app roles for enterprise applications
- Configure and manage user and admin consent
- Create and manage application collections

Plan and implement app registrations

- Plan for app registrations
- Create app registrations
- Configure app authentication
- Configure API permissions
- Create app roles

Manage and monitor app access by using Microsoft Defender for Cloud Apps

- Configure and analyze cloud discovery results by using Defender for Cloud Apps
- Configure connected apps

- Implement application-enforced restrictions
- Configure Conditional Access app control
- Create access and session policies in Defender for Cloud Apps
- Implement and manage policies for OAuth apps
- Manage the Cloud app catalog

Plan and automate identity governance (20–25%)

Plan and implement entitlement management in Microsoft Entra

- Plan entitlements
- Create and configure catalogs
- Create and configure access packages
- Manage access requests
- Implement and manage terms of use (ToU)
- Manage the lifecycle of external users
- Configure and manage connected organizations

Plan, implement, and manage access reviews in Microsoft Entra

- Plan for access reviews
- Create and configure access reviews
- Monitor access review activity
- Manually respond to access review activity

Plan and implement privileged access

- Plan and manage Microsoft Entra roles in Microsoft Entra Privileged Identity Management (PIM), including settings and assignments
- Plan and manage Azure resources in PIM, including settings and assignments

- Plan and configure groups managed by PIM
- Manage the PIM request and approval process
- Analyze PIM audit history and reports
- Create and manage break-glass accounts

Monitor identity activity by using logs, workbooks, and reports

- Review and analyze sign-in, audit, and provisioning logs by using the Microsoft Entra admin center
- Configure diagnostic settings, including configuring destinations such as Log Analytics workspaces, storage accounts, and event hubs
- Monitor Microsoft Entra ID by using KQL queries in Log Analytics
- Analyze Microsoft Entra ID by using workbooks and reporting
- Monitor and improve the security posture by using Identity Secure Score