Exam SC-300: Microsoft Identity and Access Administrator – Skills Measured

Audience Profile

The Microsoft Identity and Access Administrator designs, implements, and operates an organization's identity and access management systems by using Azure AD. They manage tasks such as providing secure authentication and authorization access to enterprise applications. The administrator provides seamless experiences and self-service management capabilities for all users. Adaptive access and governance are core elements to the role. This role is also responsible for troubleshooting, monitoring, and reporting for the identity and access environment.

The Identity and Access Administrator may be a single individual or a member of a larger team. This role collaborates with many other roles in the organization to drive strategic identity projects to modernize identity solutions, to implement hybrid identity solutions, and to implement identity governance.

Skills Measured

NOTE: The bullets that appear below each of the skills measured are intended to illustrate how we are assessing that skill. This list is not definitive or exhaustive.

NOTE: Most questions cover features that are General Availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Implement an identity management solution (25-30%)

Implement initial configuration of Azure Active Directory

- configure and manage Azure AD directory roles
- configure and manage custom domains
- configure and manage device registration options
- configure delegation by using administrative units
- configure tenant-wide settings

Create, configure, and manage identities

- create, configure, and manage users
- create, configure, and manage groups
- manage licenses

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)

Implement and manage hybrid identity

- implement and manage Azure Active Directory Connect (AADC)
- implement and manage Password Hash Synchronization (PHS)
- implement and manage Pass-Through Authentication (PTA)
- implement and manage seamless Single Sign-On (SSO)
- implement and manage Federation excluding manual ADFS deployments
- implement and manage Azure Active Directory Connect Health
- troubleshoot synchronization errors

Implement an authentication and access management solution (25-30%)

Plan and implement Azure Multifactor Authentication (MFA)

- plan Azure MFA deployment (excluding MFA Server)
- implement and manage Azure MFA settings
- manage MFA settings for users

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

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)
- testing and troubleshooting conditional access policies
- implement application controls
- implement session management
- configure smart lockout thresholds

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

Implement Access Management for Apps (10-15%)

Plan, implement, and monitor the integration of Enterprise Apps for Single Sign-On (SSO)

- implement and configure consent settings
- discover apps by using MCAS or ADFS app report
- design and implement access management for apps
- design and implement app management roles
- monitor and audit access / Sign-Ons to Azure Active Directory integrated enterprise applications
- implement token customizations
- integrate on-premises apps by using Azure AD application proxy
- integrate custom SaaS apps for SSO
- configure pre-integrated (gallery) SaaS apps
- implement application user provisioning

Implement app registrations

- plan your line of business application registration strategy
- implement application registrations
- configure application permissions
- implement application authorization
- plan and configure multi-tier application permissions

Plan and implement an Identity Governance Strategy (25-30%)

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

Plan, implement, and manage access reviews

- plan for access reviews

- create access reviews for groups and apps
- monitor access review findings
- manage licenses for access reviews
- automate access review management tasks
- configure recurring access reviews

Plan and implement privileged access

- define a privileged access strategy for administrative users (resources, roles, approvals, 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 break-glass accounts

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
- review Azure AD activity by using Log Analytics / Azure Sentinel, excluding KQL use
- analyze Azure Active Directory workbooks / reporting
- configure notifications