Identity and Access Administrator (SC-300) Study Notes

SC-300 · Microsoft · CertStud

Implement and manage user identities (22%)

At roughly 20–25% weight, this domain covers day-to-day Microsoft Entra identity administration — tenants, users, groups, roles, and hybrid sync.

Domains, branding, and tenant basics

- Add and verify custom domains (TXT/MX) before using them for UPNs
- Set a verified domain as primary so new users avoid onmicrosoft.com UPNs
- Configure company branding for the Entra sign-in experience
- Know tenant properties, group settings, and privacy contacts

Roles and administrative units

- Prefer least-privilege built-in roles (e.g., Helpdesk Administrator) over Global Administrator
- Create custom roles when built-in permissions are too broad
- Scope role assignments with administrative units for regional or departmental admins
- Use dynamic AU membership when department attributes drive scope

Groups, attributes, and hybrid

- Security groups for role/access assignment; Microsoft 365 groups for collaboration
- Dynamic membership rules for automatic group population
- Custom security attributes for searchable business metadata
- Microsoft Entra Connect Sync vs Cloud Sync; soft-match vs hard-match linking
- Entra join, hybrid join, and registered device options

Implement authentication and access management (28%)

The heaviest domain (~25–30%). Focus on authentication methods, Conditional Access design, risk-based policies, and enterprise app access.

Authentication methods

- MFA registration campaigns and method policies
- Passwordless: Authenticator passwordless, FIDO2, Windows Hello for Business
- SSPR with password writeback for hybrid users
- Password protection / banned password lists and smart lockout
- Certificate-based authentication with trusted CA bindings

Conditional Access and risk

Control	What to know
Assignments	Users/groups, cloud apps, directory roles; exclude break-glass accounts
Conditions	Sign-in risk, user risk, device platform, location, client apps
Grant	Require MFA, compliant device, hybrid join, authentication strength
Session	Sign-in frequency, persistent browser, app-enforced restrictions
ID Protection	User risk and sign-in risk policies; remediation and investigation

Apps and secure access

- Enterprise apps: SAML/OIDC, Users and groups assignment, app roles
- Consent and admin consent workflows
- Global Secure Access concepts where in scope
- Defender for Cloud Apps session/access policies for monitored apps

Plan and implement workload identities (25%)

Cover authenticating apps and Azure resources without embedding user passwords — managed identities, app registrations, and federation.

App identity building blocks

- App registration vs enterprise application (service principal) relationship
- Delegated vs application permissions; admin consent requirements
- Client secrets vs certificates — prefer certificates; rotate and expire secrets
- Redirect URIs, exposure of API scopes, and multi-tenant apps

Managed identities and federation

- System-assigned vs user-assigned managed identities
- Prefer managed identity over a user account for Azure resource access (e.g., Key Vault)
- Workload identity federation for GitHub Actions / external IdPs without long-lived secrets
- Application Proxy for publishing on-prem apps with Entra auth

Plan and automate identity governance (25%)

Close the loop on least privilege over time — JIT elevation, access packages, reviews, and identity monitoring.

Privileged Identity Management

- Eligible vs active role assignments
- Activation requirements: MFA, justification, approval, ticket
- Just-in-time elevation and time-bound access
- Access reviews of privileged role assignments

Entitlement management and reviews

- Catalogs hold resources (groups, apps, SharePoint sites)
- Access packages define who can request what and for how long
- Connected organizations for B2B package requests
- Access reviews for group membership, apps, and access packages
- Terms of use attached to Conditional Access or packages
- Lifecycle workflows for joiner/mover/leaver automation

Monitoring

- Sign-in and audit logs in Microsoft Entra
- Diagnostic settings to Log Analytics / Event Hubs / Storage
- Workbooks and reports for identity activity trends
- PIM audit history for privileged activations

Official exam objectives and domain weights. Practice at certstud.com/certifications/microsoft/sc-300/practice