Exam MS-100: Microsoft 365 Identity and Services – Skills Measured

Design and implement Microsoft 365 services (25-30%)

Manage domains

- add and configure additional domains
- configure user identities for new domain name
- configure workloads for new domain name
- design domain name configuration
- set primary domain name
- verify custom domain

Plan a Microsoft 365 implementation

- plan for Microsoft 365 on-premises Infrastructure
- plan identity and authentication solution

Setup Microsoft 365 tenancy and subscription

- configure subscription and tenant roles and workload settings
- evaluate Microsoft 365 for organization
- plan and create tenant
- upgrade existing subscriptions to Microsoft 365
- monitor license allocations

Manage Microsoft 365 subscription and tenant health

- manage service health alerts
- create & manage service requests
- create internal service health response plan
- monitor service health
- configure and review reports, including BI, OMS, and Microsoft 365 reporting
- schedule and review security and compliance reports
- schedule and review usage metrics

Plan migration of users and data

- identify data to be migrated and method
- identify users and mailboxes to be migrated and method
• plan migration of on-prem users and groups
• import PST Files

Manage user identity and roles (35-40%)

Design identity strategy

• evaluate requirements and solution for synchronization
• evaluate requirements and solution for identity management
• evaluate requirements and solution for authentication

Plan identity synchronization by using Azure AD Connect

• design directory synchronization
• implement directory synchronization with directory services, federation services, and Azure endpoints

Manage identity synchronization by using Azure AD Connect

• monitor Azure AD Connect Health
• manage Azure AD Connect synchronization
• configure object filters
• configure password sync
• implement multi-forest AD Connect scenarios

Manage Azure AD identities

• plan Azure AD identities
• implement and manage Azure AD self-service password reset
• manage access reviews
• manage groups
• manage passwords
• manage product licenses
• manage users
• perform bulk user management

Manage user roles

• plan user roles
• allocate roles in workloads
• configure administrative accounts
• configure RBAC within Azure AD
• delegate admin rights
• manage admin roles
• manage role allocations by using Azure AD
• plan security and compliance roles for Microsoft 365

Manage access and authentication (20-25%)

Manage authentication

• design authentication method
• configure authentication
• implement authentication method
• manage authentication
• monitor authentication

Implement Multi-Factor Authentication (MFA)

• design an MFA solution
• configure MFA for apps or users
• administer MFA users
• report MFA utilization

Configure application access

• configure application registration in Azure AD
• configure Azure AD application proxy
• publish enterprise apps in Azure AD

Implement access for external users of Microsoft 365 workloads

• create B2B accounts
• create guest accounts
• design solutions for external access

Plan Office 365 workloads and applications (10-15%)

Plan for Office 365 workload deployment

• identify hybrid requirements
• plan connectivity and data flow for each workload
• plan for Microsoft 365 workload connectivity
• plan migration strategy for workloads

Plan Office 365 applications deployment
- manage Office 365 software downloads
- plan for Office 365 apps
- plan for Office 365 Pro plus apps updates
- plan for Office 365 Pro plus connectivity
- plan for Office online
- plan Office 365 Pro plus deployment