MS-102: Microsoft 365 Administrator

Content

Module 1: Configure Your Microsoft 365 Experience

- Configure your organization's profile and manage subscriptions and services.
- Ensure your Microsoft Entra tenant meets business needs.

Module 2: Manage Users, Licenses, and Mail Contacts

- Choose and manage user identity models.
- Create, recover, and bulk-manage user accounts.
- Manage mail contacts via Exchange admin center and PowerShell.

Module 3: Manage Groups in Microsoft 365

- Understand and manage different group types.
- Create and manage groups through various tools.

Module 4: Add a Custom Domain

- Consider factors and plan DNS zones and records for custom domains.
- Add a custom domain to Microsoft 365.

Module 5: Configure Client Connectivity

- Use Autodiscover for Outlook connections.
- Identify required DNS records and connectivity protocols.
- Troubleshoot connectivity issues.

Module 6: Configure Administrative Roles

- Understand Azure RBAC and common admin roles.
- Delegate roles, manage permissions, and use Privileged Identity Management.

Module 7: Manage Tenant Health and Services

- Monitor service health, develop incident response plans, and request Microsoft support.

Module 8: Deploy Microsoft 365 Apps for Enterprise

- Configure deployment strategies and manage updates for Microsoft 365 Apps.

Module 9: Analyze Workplace Data with Microsoft Viva Insights

- Utilize insights for improving collaboration, identifying stressors, and assessing work culture.

Module 10: Explore Identity Synchronization

- Understand authentication models and directory synchronization.

Module 11: Prepare for Identity Synchronization

- Configure Azure AD and plan directory synchronization.

Module 12: Implement Directory Synchronization Tools

- Set up and monitor Microsoft Entra Connect Sync and Cloud Sync.

Module 13: Manage Synchronized Identities

- Ensure efficient synchronization, manage groups, and use Identity Manager.

Module 14: Manage Secure User Access

- Configure password policies, self-service management, MFA, and conditional access.

Module 15: Examine Threat Vectors and Data Breaches

- Understand attack methods, mitigate breaches, and prevent data exfiltration.

Module 16: Explore Zero Trust Security Model

- Implement Zero Trust principles and Microsoft's strategy.

Module 17: Explore Security Solutions in Microsoft Defender XDR

- Utilize Microsoft Defender for email, identity, endpoint protection, and Threat Intelligence.

Module 18: Examine Microsoft Secure Score

- Use Secure Score to identify security gaps and actions to improve security.

Module 19: Examine Privileged Identity Management

- Manage and monitor access to resources and use Privileged Access Management.

Module 20: Examine Microsoft Entra ID Protection

- Protect identities, enable policies, and manage security breaches.

Module 21: Examine Email Protection in Microsoft 365

- Utilize Exchange Online Protection to safeguard against spam and malware.

Module 22: Enhance Email Protection with Microsoft Defender for Office 365

- Use Safe Attachments and Safe Links features for added security.

Module 23: Manage Safe Attachments

- Create and configure Safe Attachments policies and manage end-user experiences.

Module 24: Manage Safe Links

- Create and configure Safe Links policies and manage user interactions.

Module 25: Explore Threat Intelligence in Microsoft Defender XDR

- Use threat intelligence, alerts, and advanced hunting for cybersecurity.

Module 26: Implement App Protection with Microsoft Defender for Cloud Apps

- Improve visibility, control, and manage cloud app protection.

Module 27: Implement Endpoint Protection with Microsoft Defender for Endpoint

- Onboard devices, manage vulnerabilities, and configure threat management.

Module 28: Implement Threat Protection with Microsoft Defender for Office 365

- Use protection stacks, Threat Explorer, and Attack Simulator.

Module 29: Examine Data Governance Solutions in Microsoft Purview

- Manage data protection, lifecycle, insider risks, and eDiscovery.

Module 30: Explore Archiving and Records Management

- Enable archive mailboxes, configure retention labels, and restore deleted data.

Module 31: Explore Retention in Microsoft 365

- Manage retention policies and labels, and understand retention principles.

Module 32: Explore Microsoft Purview Message Encryption

- Configure message encryption and branding templates.

Module 33: Explore Compliance in Microsoft 365

- Manage risks and compliance with Microsoft Purview and Compliance Manager.

Module 34: Implement Microsoft Purview Insider Risk Management

- Create and manage insider risk policies and alerts.

Module 35: Implement Microsoft Purview Information Barriers

- Restrict or allow communications and collaborations with information barriers.

Module 36: Explore Microsoft Purview Data Loss Prevention

- Manage DLP policies and monitor data protection.

Module 37: Implement Microsoft Purview Data Loss Prevention

- Create and manage custom DLP policies and notifications.

Module 38: Implement Data Classification of Sensitive Information

- Develop a data classification framework and use trainable classifiers.

Module 39: Explore Sensitivity Labels

- Understand and configure sensitivity labels for data protection.

Module 40: Implement Sensitivity Labels

- Create, configure, and publish sensitivity labels and manage label policies.