MD-102: Endpoint Administrator (16 Hours)

Overview

This instructor led online training course prepares students for MD-102 exam, which aligns to the MDAA (Modern Desktop Administrator Associate) certification. This course includes a deep dive into deploying windows, managing identity and compliance, managing applications, implementation and managing endpoints via Microsoft Intune, Windows Autopilot, and Microsoft Defender, and more.

Skills Learned

After completing this online training course, students will be able to:

- Implement a Windows client deployment by using Windows Autopilot, Microsoft Deployment Toolkit (MDT)
- Implement compliance policies and manage devices in Intune
- Manage Microsoft Defender for Endpoint & in Windows client
- Deploy a Windows client
- Configure remote management
- Implement endpoint protection
- Deploy and update apps
- Implement app protection and configuration policies

Audience Profile

This course is for Endpoint Administrators, Microsoft 365 Administrators, and Windows Administrators.

Prerequisites

None.

Course Outline

1. Preparing for a Windows client deployment

- Select a deployment tool based on requirements
- Choose between migrate and rebuild
- Choose an imaging and/or provisioning strategy
- Select a Windows edition based on requirements
- Implement subscription-based activation

2. Plan and implement a Windows client deployment by using Windows Autopilot

- Configure device registration for Autopilot
- Create, validate, and assign deployment profiles
- Set up the Enrollment Status Page (ESP)
- Deploy Windows devices by using Autopilot

3. Plan and implement a Windows client deployment by using the Microsoft Deployment Toolkit (MDT)

- Plan and implement an MDT deployment infrastructure
- Create, manage, and deploy images
- Monitor and troubleshoot a deployment
- Plan and configure user state migration

4. Configure remote management

- Configure Remote Help in Intune
- Configure Remote Desktop on a Windows client
- Configure the Windows Admin Center
- Configure PowerShell remoting and Windows Remote Management (WinRM)

5. Manage identity

- Implement user authentication on Windows devices, including Windows Hello for Business, passwordless, and tokens
- Manage role-based access control (RBAC) for Intune
- Register devices in and join devices to Azure AD
- Implement the Intune Connector for Active Directory
- Manage the membership of local groups on Windows devices
- Implement and manage Local Administrative Passwords Solution (LAPS) for Azure AD

6. Implement compliance policies for all supported device platforms by using Intune

- Specify compliance policies to meet requirements
- Implement compliance policies
- Implement Conditional Access policies that require a compliance status
- Manage notifications for compliance policies
- Monitor device compliance
- Troubleshoot compliance policies

7. Manage the device lifecycle in Intune

- Configure enrollment settings
- Configure automatic and bulk enrollment, including Windows, Apple, and Android
- Configure policy sets
- Restart, retire, or wipe devices

8. Manage device configuration for all supported device platforms by using Intune

- Specify configuration profiles to meet requirements
- Implement configuration profiles
- Monitor and troubleshoot configuration profiles
- Configure and implement Windows kiosk mode
- Configure and implement profiles on Android devices
- Plan and implement Microsoft Tunnel for Intune

9. Monitor devices

- Monitor devices by using Intune
- Monitor devices by using Azure Monitor
- Analyze and respond to issues identified in Endpoint analytics and Adoption Score

10. Manage device updates for all supported device platforms by using Intune

- Plan for device updates
- Create and manage update policies by using Intune
- Manage Android updates by using configuration profiles
- Monitor updates
- Troubleshoot updates in Intune
- Configure Windows client delivery optimization by using Intune
- Create and manage update rings by using Intune

11. Implement endpoint protection for all supported device platforms

- Implement and manage security baselines in Intune
- Create and manage configuration policies for Endpoint security including antivirus, encryption, firewall, endpoint detection and response (EDR), and attack surface reduction (ASR)
- Onboard devices to Defender for Endpoint
- Implement automated response capabilities in Defender for Endpoint
- Review and respond to device issues in the Microsoft Defender Vulnerability Management dashboard

12. Deploy and update apps for all supported device platforms

- Deploy apps by using Intune
- Configure Microsoft 365 Apps deployment by using the Microsoft Office Deployment Tool or Office Customization Tool (OCT)
- Manage Microsoft 365 Apps by using the Microsoft 365 Apps admin center
- Deploy Microsoft 365 Apps by using Intune
- Configure policies for Office apps by using Group Policy or Intune
- Deploy apps to platform-specific app stores by using Intune

13. Plan and implement app protection and app configuration policies

- Plan and implement app protection policies for iOS and Android
- Manage app protection policies
- Implement Conditional Access policies for app protection policies
- Plan and implement app configuration policies for managed apps and managed devices
- Manage app configuration policies