AZ-140T00: Configuring and Operating Microsoft Azure Virtual Desktop

Course Duration: 32 Hours (4 Days)

Overview

The AZ-140T00: Configuring and Operating Microsoft Azure Virtual Desktop course is designed to equip learners with the expertise to implement, plan, and maintain a Microsoft Azure Virtual Desktop infrastructure. Through a series of five modules, participants will gain a thorough understanding of the Windows Virtual Desktop architecture, design considerations for Identity and profile management, and the deployment processes for both Azure Active Directory Domain Services (Azure AD DS) and Active Directory Domain Services (AD DS).Learners will also delve into managing networking, storage, Host pools, Session hosts, and images, and will explore how to automate deployment using Azure Resource Manager templates and PowerShell. The course covers crucial aspects of Access management and security, including configuring Conditional Access policies. The training provides insights on managing user environments, implementing FSLogix, Configuring user experience settings, and App installation. Additionally, it emphasizes monitoring, performance management, and implementing autoscaling. Completing this course will empower individuals with the skills necessary to ensure smooth operation and optimization of Azure Virtual Desktop environments, which is essential for businesses leveraging cloud desktops and apps.

Audience Profile

The AZ-140T00 course is designed for IT professionals focusing on virtual desktop infrastructure using Microsoft Azure. Target audience for the course includes:

- IT Administrators and System Administrators responsible for managing virtual desktop experiences and remote apps.
- Microsoft Azure Administrators tasked with implementing and managing virtual desktop infrastructure.
- Network Engineers oversee the implementation and management of networking for Windows Virtual Desktop (WVD).
- Security Professionals in charge of access management and security for WVD.
- Desktop Support Technicians facilitating end-user support and app management on WVD session hosts.
- Cloud Architects is involved in designing and planning WVD architecture.
- IT Professionals interested in learning about Azure Virtual Desktop deployment, scaling, and management.
- Disaster Recovery and Business Continuity Specialists focusing on WVD infrastructure.
- IT Professionals looking to automate WVD management tasks and monitor performance.

- Application Developers and DevOps Engineers interested in application packaging and deployment for WVD.

Course Syllabus

Module 1: Plan and implement an Azure Virtual Desktop infrastructure (40–45%)

Plan, implement, and manage networking for Azure Virtual Desktop

- Assess network capacity and speed requirements for Azure Virtual Desktop
- Design network configuration for session hosts to meet requirements for Azure Virtual Desktop
- Plan and implement Remote Desktop Protocol (RDP) Shortpath and quality of service (QoS) policies
- Plan and implement an Azure Private Link solution for Azure Virtual Desktop
- Monitor and troubleshoot network connectivity

Plan and implement storage for Azure Virtual Desktop user data

- Plan storage for Azure Virtual Desktop user data
- Implement storage for FSLogix components
- Implement storage accounts for Azure Virtual Desktop
- Implement file shares for Azure Virtual Desktop
- Implement Azure NetApp Files for Azure Virtual Desktop

Plan host pools and session hosts

- Recommend resource groups, subscriptions, and management groups for Azure Virtual Desktop resources
- Recommend an operating system (OS) for Azure Virtual Desktop session hosts
- Recommend an appropriate licensing model for Azure Virtual Desktop based on requirements
- Plan a host pool architecture
- Design an Azure Virtual Desktop configuration for performance requirements
- Design an Azure Virtual Desktop configuration for Azure Virtual Machines capacity requirements

Implement host pools and session hosts

- Create host pools and session hosts by using the Azure portal
- Automate creation of Azure Virtual Desktop hosts and host pools by using PowerShell, Azure CLI, Azure Resource Manager templates (ARM templates), and Bicep

- Configure host pool and session host settings
- Apply a Windows client or Windows Server license to a session host

Create and manage session host images

- Create an image manually
- Create an image by using Azure virtual machine Image Builder
- Modify an image
- Plan and implement lifecycle management for images
- Apply OS and application updates to an image
- Create a session host by using a custom image
- Plan and implement image storage, including Compute Gallery

Module 2: Plan and implement identity and security (15–20%)

Plan and implement identity integration

- Select an identity scenario for Azure Virtual Desktop, including Active Directory Domain Services (AD DS), Microsoft Entra ID, and Microsoft Entra Domain Services
- Specify requirements to configure the Azure Virtual Desktop session host for an identity scenario
- Plan and implement Azure roles and role-based access control (RBAC) for Azure Virtual Desktop
- Plan and implement Conditional Access policies for connections to Azure Virtual Desktop
- Plan and implement authentication options in Azure Virtual Desktop, including password less, smart card, and multifactor authentication
- Manage roles, groups, and rights assignments on Azure Virtual Desktop session hosts
- Configure single sign-on

Plan and implement security

- Plan, implement, and manage security for Azure Virtual Desktop session hosts by using Microsoft Defender for Cloud
- Configure session host protection by using Microsoft Defender Antivirus
- Configure session host protection by using Microsoft Defender for Endpoint, including onboarding and scanning options
- Implement and manage network security for connections to Azure Virtual Desktop, including user defined routes (UDRs), network security groups (NSGs), and Azure Firewall
- Configure Azure Bastion or just-in-time (JIT) for administrative access to session hosts
- Plan and implement Windows threat protection features on Azure Virtual Desktop session hosts, including Windows Defender Application Control and Controlled Folder Access

- Plan for and implement Confidential VM and Trusted Launch security features for Azure Virtual Desktop session host provisioning

Module 3: Plan and implement user environments and apps (20–25%)

Plan and implement FSLogix

- Recommend FSLogix configuration
- Configure FSLogix Profile Containers
- Configure FSLogix Office Containers
- Configure FSLogix Cloud Cache
- Implement FSLogix application masking

Plan and implement user experience and client settings

- Choose an Azure Virtual Desktop client
- Choose a deployment method for the client
- Deploy and troubleshoot Azure Virtual Desktop clients
- Configure device redirection
- Configure multimedia redirection
- Configure printing and Universal Print
- Configure user settings through Microsoft Intune policies or Group Policy
- Configure Remote Desktop Protocol (RDP) properties on a host pool
- Configure session timeout properties
- Implement the Start Virtual Machine on Connect feature
- Assign and unassign personal desktops for users

Install and configure apps on a session host

- Choose a method for deploying an app to Azure Virtual Desktop
- Create and configure an application group
- Assign users to application groups
- Publish an application as a RemoteApp
- Implement and manage Microsoft 365 apps on Azure Virtual Desktop session hosts
- Implement and manage OneDrive, including multisession environments
- Implement and manage Microsoft Teams, including the Remote Desktop WebRTC Redirector Service
- Implement and manage browsers for Azure Virtual Desktop sessions
- Configure dynamic application delivery by using app attach or MSIX app attach
- Create an application package for app attach or MSIX app attach

Module 4: Monitor and maintain an Azure Virtual Desktop infrastructure (10– 15%)

Monitor and manage Azure Virtual Desktop services

- Configure log collection and analysis for Azure Virtual Desktop session hosts
- Monitor Azure Virtual Desktop by using Azure Monitor
- Customize Azure Monitor workbooks for Azure Virtual Desktop Insights
- Optimize session host capacity and performance
- Implement autoscaling in host pools
- Monitor and manage active sessions and application groups

Plan and implement updates, backups, and disaster recovery

- Recommend an update strategy for session hosts
- Plan and implement a disaster recovery plan for Azure Virtual Desktop
- Plan for multi-region implementation
- Design and implement a backup strategy for Azure Virtual Desktop
- Configure backup and restore for FSLogix user profiles, personal virtual desktop infrastructures (VDIs), and golden images