Exam AZ-140: Configuring and Operating Windows Virtual Desktop on Microsoft Azure (beta)

Introduction

Configuring and Operating Windows Virtual Desktop on Microsoft Azure (Exam AZ-140) certification examination is ideal for professionals who want to gain subject matter expertise in planning, delivering, and managing virtual desktop experiences and remote apps, for any device, on Azure. The AZ-140 exam successfully measures the candidate's ability to plan a Windows Virtual Desktop architecture; implement the Windows Virtual Desktop infrastructure; manage access and security; manage user environments and apps, and hence, monitor and maintain a Windows Virtual Desktop infrastructure.

Moreover, with Certbazar's exclusive training course, the candidates will also get a deep understanding of Azure technologies, including virtualization, networking, identity, storage, backups, resilience, and most important of all, disaster recovery.

Course Outline

MODULE 1: Plan a Windows Virtual Desktop architecture (10-15%)

- Design the Windows Virtual Desktop architecture
  - assess existing physical and virtual desktop environments
  - assess network capacity and speed requirements for Windows Virtual Desktop
  - recommend an operating system for a Windows Virtual Desktop implementation
  - plan and configure name resolution for Active Directory (AD) and Azure Active Directory Domain Services (Azure AD DS)
  - plan a host pools architecture
  - recommend resource groups, subscriptions, and management groups
  - configure a location for the Windows Virtual Desktop metadata
  - calculate and recommend a configuration for performance requirements
  - calculate and recommend a configuration for Azure Virtual Machine capacity requirements

- Design for user identities and profiles
  - select an appropriate licensing model for Windows Virtual Desktop based on requirements
  - recommend an appropriate storage solution (including Azure NetApp Files versus Azure Files)
  - plan for Windows Virtual Desktop client deployment
  - plan for user profiles
  - recommend a solution for network connectivity
  - plan for Azure AD Connect for user identities

MODULE 2: Implement a Windows Virtual Desktop infrastructure (25-30%)

- Implement and manage networking for Windows Virtual Desktop
  - implement Azure virtual network connectivity
  - manage connectivity to the internet and on-premises networks
  - implement and manage network security
  - manage Windows Virtual Desktop session hosts by using Azure Bastion
  - monitor and troubleshoot network connectivity
  -
- Implement and manage storage for Windows Virtual Desktop
  - configure storage for FSLogix components
  - configure storage accounts
  - configure disks
  - create file shares

- Create and configure host pools and session hosts
  - create a host pool by using the Azure portal

- automate the creation of Windows Virtual Desktop host and host pools by using PowerShell, Command-Line Interface (CLI), and Azure Resource Manager templates
- create a host pool based on Windows client or Windows Server session hosts
- configure host pool settings
- manage to license for session hosts that run Windows client or Windows Server
- assign users to host pools
- apply OS and application updates to a running Windows Virtual Desktop host
- apply security and compliance settings to session hosts

- Create and manage session host images
  - create a gold image
  - modify a session host image
  - install language packs in Windows Virtual Desktop
  - deploy a session host by using a custom image
  - plan for image update and management
  - create and use a Shared Image Gallery
  - troubleshoot OS issues related to Windows Virtual Desktop

MODULE 3: Manage access and security (10-15%)

- Manage access
  - plan and implement Azure roles and role-based access control (RBAC) for Windows Virtual Desktop
  - manage local roles, groups, and rights assignment on Windows Virtual Desktop session hosts
  - configure user restrictions by using Azure AD group policies and AD policies

- Manage security
  - plan and implement Conditional Access policies for connections to Windows Virtual Desktop
  - plan and implement multifactor authentication in Windows Virtual Desktop
  - manage security by using Azure Security Center
  - configure Microsoft Defender Antivirus for session hosts

MODULE 4: Manage user environments and apps (20-25%)

- Implement and manage FSLogix
  - plan for FSLogix
  - install and configure FSLogix
  - configure Profile Containers
  - configure Cloud Cache
  - migrate user profiles to FSLogix

- Configure user experience settings
  - configure Universal Print
  - configure user settings through group policies and Endpoint Manager policies
  - configure persistent and non-persistent desktop environments
  - configure Remote Desktop Protocol (RDP) properties on a host pool
  - configure session timeout properties
  - troubleshoot user profile issues
  - troubleshoot Windows Virtual Desktop clients

- Install and configure apps on a session host
  - configure dynamic application delivery by using MSIX App Attach
  - implement application masking
  - deploy an application as a RemoteApp
  - implement and manage OneDrive for Business for a multi-session environment
  - implement and manage Microsoft Teams AV Redirect
  - implement and manage browsers and internet access for Windows Virtual Desktop sessions
  - create and configure an application group
  - troubleshoot application issues related to Windows Virtual Desktop

MODULE 5: Monitor and maintain a Windows Virtual Desktop infrastructure (20-25%)

- Plan and implement business continuity and disaster recovery
  - plan and implement a disaster recovery plan for Windows Virtual Desktop
  - design a backup strategy for Windows Virtual Desktop
  - configure backup and restore for FSLogix user profiles, personal virtual desktop infrastructures (VDIs), and golden images

- Automate Windows Virtual Desktop management tasks
    - configure automation for Windows Virtual Desktop
    - automate the management of host pools, session hosts, and user sessions by using PowerShell and Azure Command-Line Interface (CLI)
    - implement autoscaling in host pools

- Monitor and manage performance and health
    - monitor Windows Virtual Desktop by using Azure Monitor
    - monitor Windows Virtual Desktop by using Azure Advisor
    - customize Azure Monitor workbooks for Windows Virtual Desktop monitoring
    - optimize session host capacity and performance
    - manage active sessions and application groups
    - monitor and optimize autoscaling results

Prerequisites

- Understanding of virtualization, networking, identity, storage, backups, resilience, and disaster recovery.
- Understanding of on-premises virtual desktop infrastructure technologies
- AZ-104T00: Microsoft Azure Administrator
- AZ-900T00: Microsoft Azure Fundamentals

Target Audience

Candidates for this exam are Microsoft Azure administrators with subject matter expertise in planning, delivering, and managing virtual desktop experiences and remote apps, for any device, on Azure.

Responsibilities for this role include deploying virtual desktop experiences and apps to Azure.

Professionals in this role deliver applications on Windows Virtual Desktop and optimize them to run in multi-session virtual environments. To deliver these experiences, they work closely with the Azure administrators and architects, along with Microsoft 365 Administrators.

Candidates for this exam should have experience in Azure technologies, including virtualization, networking, identity, storage, backups, resilience, and disaster recovery. They should understand on-premises virtual desktop infrastructure technologies as they relate to migrating to Windows Virtual Desktop. These professionals use the Azure portal and Azure Resource Manager templates to accomplish many tasks. This role may use PowerShell and Azure Command-Line Interface (CLI) for more efficient automation.

Candidates for this exam must have expert Azure administration skills.

Duration

32 Hours