Configuring and Operating Microsoft Azure Virtual Desktop

Course AZ-140T00: 4 days; Instructor-Led

Introduction

This course teaches Azure administrators how to plan, deliver, and manage virtual desktop experiences and remote apps, for any device, on Azure. Lessons include implementing and managing networking for Azure Virtual Desktop, configuring host pools and session hosts, creating session host images, implementing, and managing FSLogix, monitoring Azure Virtual Desktop performance and health, and automating Azure Virtual Desktop management tasks. Students will learn through a mix of demonstrations and hands-on lab experiences deploying virtual desktop experiences and apps on Azure Virtual Desktop and optimizing them to run in multi-session virtual environments. Candidates of this course must have solid Azure administration skills. This course assumes prior experience, including virtualization, networking, identity, storage, backup and restore, and disaster recovery. Students should have knowledge of on-premises virtual desktop infrastructure technologies as they relate to migrating to Azure Virtual Desktop. Students are expected to have used the tools common to the Azure environment, such as the Azure PowerShell and Cloud Shell.

Audience

Students for AZ-140: Configuring and Operating Microsoft Azure Virtual Desktop are interested in delivering applications on Azure Virtual Desktop and optimizing them to run in multi-session virtual environments. As an Azure Virtual Desktop administrator, you will closely with the Azure Administrators and Architects, along with Microsoft 365 Administrators. Azure Virtual Desktop administrator responsibilities include planning, deploying, packaging, updating, and maintaining the Azure Virtual Desktop infrastructure. They also create session host images, implement and manage FSLogix, monitor Azure Virtual Desktop performance, and automate Azure Virtual Desktop management tasks.

Job role: Administrator
Preparation for exam: AZ-140

Course Outline

Module 1: Azure Virtual Desktop Architecture
Azure Virtual Desktop manages the infrastructure and brokering components, while customers manage their own desktop host virtual machines (VMs) and clients. Microsoft manages the Remote Connection Gateway, and Connection Broker services as part of Azure.

In this module, you will:

- Create and run a flow. Explain the Azure Virtual Desktop components.
- Describe the Azure Virtual Desktop architecture.
- Choose between personal and pooled desktops.
- Identify the Azure limitations for Azure Virtual Desktop.
- Describe the options for Azure Virtual Desktop pricing.
-

Lessons

- Introduction
- Azure Virtual Desktop for the enterprise
- Azure Virtual Desktop components
- Personal and pooled desktops
- Service updates for Azure Virtual Desktop desktops
- Azure limitations for Azure Virtual Desktop
- Virtual machine sizing for Azure Virtual Desktop
- Azure Virtual Desktop pricing

Module 2: Design the Azure Virtual Desktop architecture
Azure Virtual Desktop design requires that you assess network capacity and speed requirements, select a load-balancing method for your Azure Virtual Desktop deployment, and choose the right Windows Desktop client.

In this module, you will:

- Assess network capacity and speed requirements for Azure Virtual Desktop.
- Determine the connection round-trip time (RTT) from a location through the Azure Virtual Desktop service.
- Recommend an operating system for an Azure Virtual Desktop implementation.
- Describe the two load-balancing methods for Azure Virtual Desktop.
- Recommendation subscriptions and management groups for Azure Virtual Desktop.
- Recommend a configuration for performance requirements.

Lessons

- Introduction
- Assess network capacity and speed requirements for Azure Virtual Desktop
- Azure Virtual Desktop Experience Estimator
- Recommend an operating system for an Azure Virtual Desktop implementation
- Balancing host pools
- Recommendations for using subscriptions and management groups
- Configure a location for the Azure Virtual Desktop metadata
- Recommend a configuration for performance requirements

Module 3: Design for user identities and profiles
Your users require access to those applications both on-premises and in the cloud. You use the Remote Desktop client for Windows Desktop to access Windows apps and desktops remotely from a different Windows device.

In this module, you will:

- Perform a test run of the new desktop flow. Select a licensing model for Azure Virtual Desktop.
- Describe personal and multi-session desktop scenarios.
- Plan a storage solution storing FSLogix profile containers.
- Plan for a Desktop client deployment
- Deploy Windows Desktop client to multiple devices.
- Describe Hybrid Identity for Azure Virtual Desktop.

Lessons

- Introduction
- Select an appropriate licensing model for Azure Virtual Desktop based on requirements
- Personal and multi-session desktop scenarios
- Recommend an appropriate storage solution
- Plan for a desktop client deployment
- Plan for Azure Virtual Desktop client deployment - Remote Desktop Protocol (RDP)
- Windows Desktop client to multiple devices
- Hybrid Identity with Azure Active Directory
- Plan for Azure Active Directory (AD) Connect for user identities

Module 4: Implement and manage networking for Azure Virtual Desktop
See how to monitor and repair health of their Azure Virtual Desktop including virtual machines, virtual networks, application gateways, and load balancers.

In this module, you will:

- Recommend a solution for Azure Virtual Desktop network connectivity.
- Implement Azure virtual network connectivity for Azure Virtual Desktop.
- Describe network security for Azure Virtual Desktop.
- Configure Azure Virtual Desktop session hosts using Microsoft Bastion.
- Monitor communication between a virtual machine and an endpoint.

Lessons

- Introduction
- Implement Azure virtual network connectivity
- Manage connectivity to the internet and on-premises networks
- Understanding Azure Virtual Desktop network connectivity
- Implement and manage network security for Azure Virtual Desktop
- Configure Azure Virtual Desktop session hosts using Azure Bastion
- Monitor and troubleshoot network connectivity for Azure Virtual Desktop
- Plan and implement Remote Desktop Protocol Shortpath
- Configure Remote Desktop Protocol Shortpath for managed networks
- Configure Windows Defender Firewall with Advanced Security for RDP Shortpath
- Plan and implement Quality of Service for Azure Virtual Desktop

Module 5: Implement and manage storage for Azure Virtual Desktop

FSLogix roams profiles in remote computing environments, such as Azure Virtual Desktop. You set up a FSLogix profile container share for a host pool using a virtual machine-based file share.

In this module, you will:

- Test the new cloud flow. Choose appropriate storage for FSLogix components.
- Configure storage for FSLogix components.
- Configure storage accounts for Azure Files.
- Configure a new managed data disk to a Windows virtual machine for Azure Virtual Desktop.
- Create file shares for a storages account for Azure Virtual Desktop.

Lessons

- Introduction
- Storage for FSLogix components
- Configure storage for FSLogix components
- Configure storage accounts
- Create file shares
- Configure disks

Module 6: Create and configure host pools and session hosts for Azure Virtual Desktop

See how to configure the assignment type of a personal desktop host pool to adjust your Azure Virtual Desktop environment to better suit your needs.

In this module, you will:

- Configure host pool assignment type.
- Automate creation of an Azure Virtual Desktop host pool using PowerShell.
- Customize Remote Desktop Protocol (RDP) properties for a host pool.
- Manage licensing for session hosts that run Windows client.

Lessons

- Introduction
- Automate creation of an Azure Virtual Desktop host pool using PowerShell
- Configure host pool assignment type
- Customize Remote Desktop Protocol (RDP) properties for a host pool
- Manage licensing for session hosts that run Windows client
- Deploying Azure AD-joined virtual machines in Azure Virtual Desktop

Module 7: Create and manage session host image for Azure Virtual Desktop

A Shared Image Gallery simplifies custom image sharing across your organization. Custom images can be used to bootstrap deployment tasks like preloading applications, application configurations, and other OS configurations.

In this module, you will:

- Create a managed VM image for an Azure Virtual Desktop-specific configuration.
- Modify a session host image.
- Plan for image update and management.
- Create and use a Shared Image Gallery (SIG) for Azure Virtual Desktop.
- Install language packs in Azure Virtual Desktop.

Lessons

- Introduction
- Create a managed virtual machine (VM) image
- Modify a session host image
- Plan for image update and management
- Create and use an Azure Compute Gallery using the portal
- Create an Azure Virtual Desktop image by using VM Image Builder
- Install Microsoft 365 Apps on a master Virtual Hard Disk image
- Install language packs in Azure Virtual Desktop

Module 8: Manage access for Azure Virtual Desktop

Azure Virtual Desktop uses Azure role-based access controls (RBAC) to assign roles to users and admins. Azure Virtual Desktop has additional roles that let you separate management roles for host pools, app groups, and workspaces.

In this module, you will:

- Describe Azure role-based access controls (RBAC) for Azure Virtual Desktop.
- Plan and implement Azure roles and RBAC for Azure Virtual Desktop.
- Describe how to configure Azure Virtual Desktop with Intune.

Lessons

- Introduction
- Role-based access control (RBAC) for Azure Virtual Desktop
- Plan and implement Azure roles and role-based access control (RBAC) for Azure Virtual Desktop
- Using Azure Virtual Desktop with Microsoft Intune
- Configuring screen capture protection for Azure Virtual Desktop

Module 9: Manage security for Azure Virtual Desktop

The Windows client for Azure Virtual Desktop integrates Azure Virtual Desktop on local machines. You'll learn the critical actions for keeping your users safe.

In this module, you will:

- Plan and implement Conditional Access policies for connections to Azure Virtual Desktop.
- Plan and implement multifactor authentication (MFA) in Azure Virtual Desktop.
- Understand Conditional Access policy components.
- Manage security by using Azure Security Center.
- Understand Microsoft Defender Antivirus for session hosts.

Lessons

- Introduction
- Plan and implement Conditional Access policies for connections to Azure Virtual Desktop
- Plan and implement multifactor authentication (MFA) in Azure Virtual Desktop
- Understand Conditional Access policy components
- Manage security by using Azure Security Center

Module 10: Implement and manage FSLogix

A user profile contains data elements about a user information like desktop settings, persistent network connections, and application settings.

In this module, you will:

- Plan for FSLogix.
- Recommend best practices for FSLogix profile containers and Azure files.
- Install FXLogix.
- Recommend storage options for FSLogix profile containers.
- Configure Cloud Cache.
- Configure Profile Containers.
- Manage Rule Sets and application masking.

Lessons

- Introduction
- Plan for FSLogix
- FSLogix profile containers and Azure files
- Install FSLogix
- Storage options for FSLogix profile containers
- Profile Container vs Office Container
- Configure Office Containers
- Installing Microsoft Office using FSLogix application containers
- Configure Cloud Cache
- Configure Profile Containers
- Create a profile container with Azure NetApp Files and capacity pool
- Manage Rule Sets and application masking

Module 11: Configure user experience settings

Persistent virtual desktops save the operating system state in between reboots. Virtual desktop provides users easy and seamless access to their assigned VMs, often with a single sign-on solution.

In this module, you will:

- Configure user settings through group policies for Azure Virtual Desktop.
- Configure user settings through Endpoint Manager policies for Azure Virtual Desktop.
- Configure session timeout properties for Azure Virtual Desktop.
- Configure device redirections for Azure Virtual Desktop.
- Configure Universal Print.
- Troubleshoot user profile issues.

Lessons

- Introduction
- Virtual desktop optimization principles
- Persistent virtual desktop environments
- Configure user settings through group policies
- Configure user settings through Endpoint Manager policies
- Configure session timeout properties
- Configure device redirections
- Configure Universal Print
- Implement the Start Virtual Machine on Connect feature
- Troubleshoot user profile issues
- Troubleshoot Azure Virtual Desktop clients

Module 12: Install and configure apps on a session host

MSIX app attach is a way to deliver MSIX applications to both physical and virtual machines. MSIX app attach is different from regular MSIX because it’s specifically for Azure Virtual Desktop.

In this module, you will:

- Describe MSIX app attach for Azure Virtual Desktop.
- Explain how MSIX app attach works.

- Set up a file share for MSIX app attach.
- Use the OneDrive sync app on Azure Virtual Desktops.
- Use Microsoft Teams on Azure Virtual Desktop.
- Publish built-in apps in Azure Virtual Desktop.

Lessons

- Introduction
- MSIX app attach
- How MSIX app attach works
- Set up a file share for MSIX app attach
- Upload MSIX images to Azure NetApp Files in Azure Virtual Desktop
- How to configure apps for users
- Using the OneDrive sync app on virtual desktops
- Using Microsoft Teams on Azure Virtual desktop
- Publish built-in apps in Azure Virtual Desktop
- Troubleshoot application issues for Azure Virtual Desktop

Module 13: Plan for disaster recovery

You can replicate your virtual machines (VMs) to the secondary location for Azure Virtual Desktop. You use Azure Site Recovery to manage replicating VMs in other Azure locations.

In this module, you will:

- Configure virtual machine (VM) replication for Azure Virtual Desktop.
- Configure FSLogix for multiple profile locations.

Lessons

- Introduction
- Disaster recovery for Azure Virtual Desktop
- Virtual machine replication
- FSLogix configuration
- Knowledge check

Module 14: Automate Azure Virtual Desktop management tasks

Azure Virtual Desktop deployment costs by scaling virtual machines (VMs). This means shutting down and deallocating session host VMs during off-peak usage hours, then turning them back on and reallocating them during peak hours.

In this module, you will:

- Describe how to scale session hosts using Azure Automation.
- Create or update an Azure Automation account.
- Create an Azure Automation Run As account.
- Create the Azure Logic App and execution schedule.

Lessons

- Introduction
- Scale session hosts using Azure Automation
- Create or update an Azure Automation account
- Create an Azure Automation Run As account
- Create the Azure Logic App and execution schedule

Module 15: Monitor and manage performance and health

For Azure Virtual Desktop issues, check Azure Advisor first. Azure Advisor will give you directions for how to solve the problem, or at least point you towards a resource that can help.

In this module, you will:

- Describe how to monitor Azure Virtual Desktop by using Azure Monitor.
- How to use Log Analytics workspace for Azure Monitor.
- How to monitor Azure Virtual Desktop by using Azure Advisor.
- How to resolve Azure Advisor recommendations.
- How to diagnose graphics performance issues.

Lessons

- Introduction
- Monitor Azure Virtual Desktop by using Azure Monitor
- Log Analytics workspace for Azure Monitor
- Monitor Azure Virtual Desktop by using Azure Advisor
- How to resolve Azure Advisor recommendations
- Diagnose graphics performance issues