Configuring Windows Server Hybrid Advanced Services

Course AZ-801T00: 4 days; Instructor-Led

Introduction

This course teaches IT Professionals to configure advanced Windows Server services using on-premises, hybrid, and cloud technologies. The course teaches IT Professionals how to leverage the hybrid capabilities of Azure, how to migrate virtual and physical server workloads to Azure IaaS, and how to secure Azure VMs running Windows Server. The course also teaches IT Professionals how to perform tasks related to high availability, troubleshooting, and disaster recovery. The course highlights administrative tools and technologies including Windows Admin Center, PowerShell, Azure Arc, Azure Automation Update Management, Microsoft Defender for Identity, Azure Security Center, Azure Migrate, and Azure Monitor.

Audience

This four-day course is intended for Windows Server Hybrid Administrators who have experience working with Windows Server and want to extend the capabilities of their on-premises environments by combining on-premises and hybrid technologies. Windows Server Hybrid Administrators who already implement and manage on-premises core technologies want to secure and protect their environments, migrate virtual and physical workloads to Azure Iaas, enable a highly available, fully redundant environment, and perform monitoring and troubleshooting.

Job role: Administrator
Preparation for exam: AZ-801

Prerequisites

Before attending this course, students must have:

- Experience with managing Windows Server operating system and Windows Server workloads in on-premises scenarios, including AD DS, DNS, DFS, Hyper-V, and File and Storage Services
- Experience with common Windows Server managemeH nt tools (implied in the first prerequisite).
- Basic knowledge of core Microsoft compute, storage, networking, and virtualiz...
- Experience and an understanding of core networking technologies such as IP addressing, name resolution, and Dynamic Host Configuration Protocol (DHCP)
- Experience working with and an understanding of Microsoft Hyper-V and basic server virtualization concepts
- An awareness of basic security best practices
- Basic understanding of security-related technologies (firewalls, encryption, multi-factor authentication, SIEM/SOAR).
- Basic knowledge of on-premises resiliency Windows Server-based compute and storage technologies (Failover Clustering, Storage Spaces).
- Basic experience with implementing and managing IaaS services in Microsoft Azure
- Basic knowledge of Azure Active Directory
- Experience working hands-on with Windows client operating systems such as Windows 10 or Windows 11
- Basic experience with Windows PowerShell

Course Outline

Module 1: Secure Windows Server user accounts

Protect your Active Directory environment by securing user accounts to least privilege and placing them in the Protected Users group. Learn how to limit authentication scope and remediate potentially insecure accounts.

In this module, you will:

- Configure and manage user accounts to limit security threats across an organization
- Apply Protected Users settings, policies, and authentication silos to protect highly privileged user accounts
- Describe and configure Windows Defender Credential Guard
- Configure Group Policy to block the use of NTLM for authentication

Lessons

- Introduction
- Configure user account rights
- Protect user accounts with the Protected Users group
- Describe Windows Defender Credential Guard
- Block NTLM authentication
- Locate problematic accounts

Module 2: Hardening Windows Server

Learn how to harden the security configuration of your Windows Server operating system environment. Secure administrative access to Privileged Access Workstations (PAWs), apply security baselines, and secure domain controllers and SMB traffic.

In this module, you will:

- Manage local administrator passwords using Local Administrator Password Solution
- Limit administrative access to Privileged Access Workstations (PAWs)
- Explain how to secure domain controllers from being compromised
- Describe how to use the Microsoft Security Compliance Toolkit to harden servers
- Secure SMB traffic using SMB encryption

Lessons

- Introduction
- Describe Local Password Administrator Solution
- Configure Privileged Access Workstations
- Secure domain controllers
- Analyze security configuration with Security Compliance Toolkit
- Secure SMB traffic

Module 3: Windows Server update management

Learn how to use Windows Server Update Services to deploy operating system updates to computers on your network. Select the appropriate deployment option and combine WSUS with Microsoft Azure Update Management to manage server updates.

In this module, you will:

- Describe the role of Windows Server Update Services (WSUS)
- Describe the WSUS update management process
- Deploy updates with WSUS

Lessons

- Introduction
- Explore Windows Update
- Outline Windows Server Update Services server deployment options
- Define Windows Server Update Services update management process
- Describe the process of Update Management

Module 4: Secure Windows Server DNS

Learn how to secure Windows Server DNS to help protect your network name resolution infrastructure and also learn how to implement DNS policies.

In this module, you will:

- Describe split-horizon DNS and explain how to implement it.
- Create DNS policies.
- Implement DNS policies.
- Describe the options for protecting the DNS server role.
- Implement DNS security.

Lessons

- Introduction
- Implement split-horizon DNS
- Create DNS policies
- Implement DNS policies
- Secure Windows Server DNS
- Implement DNSSEC

Module 5: Implement Windows Server IaaS VM network security

In this module, you will focus on how to improve the network security for Windows Server infrastructure as a service (IaaS) virtual machines (VMs) and how to diagnose network security issues with those VMs.

In this module, you will:

- Implement Network Security Groups (NSGs) with Windows Server IaaS VMs.
- Implement adaptive network hardening.
- Implement Azure Firewall.
- Implement Windows Defender Firewall in Windows Server IaaS VMs.
- Choose an appropriate filtering solution.
- Capture network traffic with Network Watcher.

Lessons

- Introduction
- Implement network security groups and Windows IaaS VMs
- Implement adaptive network hardening
- Implement Azure Firewall and Windows IaaS VMs
- Implement Windows firewall with Windows Server IaaS VMs
- Choose the appropriate filtering solution
- Deploy and configure Azure firewall using the Azure portal
- Capture network traffic with network watcher
- Log network traffic to and from a VM using the Azure portal

Module 6: Audit the security of Windows Server IaaS Virtual Machines

You'll learn about Azure Security Center and how to onboard Windows Server computers to Security Center. You'll also learn about Azure Sentinel, security information and event management (SIEM), and security orchestration, automation and response (SOAR).

In this module, you will:

- Describe Azure Security Center.
- Enable Azure Security Center in hybrid environments.
- Onboard Windows Server computers to Azure Security Center.
- Implement and assess security policies.
- Describe Azure Sentinel.
- Implement SIEM and SOAR.
- Protect your resources with Azure Security Center.

Lessons

- Introduction
- Describe Azure Security Center
- Enable Azure Security Center in hybrid environments
- Implement and assess security policies
- Protect your resources with Azure Security Center
- Implement Azure Sentinel

Module 7: Manage Azure updates

You'll be able to enable Azure Update Management, deploy updates, review an update assessment, and manage updates for your Azure VMs.

In this module, you will:

- Describe Azure updates.
- Enable Update Management.
- Deploy updates.
- Review an update assessment.
- Manage updates for your Azure VMs.

Lessons

- Introduction
- Describe update management
- Enable update management
- Deploy updates
- View update assessments
- Manage updates for your Azure Virtual Machines

Module 8: Create and implement application allowlists with adaptive application control

You'll be able to implement Adaptive application controls within your organization to protect your Windows Server IaaS VMs.

In this module, you will:

- Enable Adaptive application controls.
- Implement adaptive application control policies.

Lessons

- Introduction
- Describe adaptive application control
- Implement adaptive application control policies

Module 9: Configure BitLocker disk encryption for Windows IaaS Virtual Machines

You'll be able to configure Azure Disk Encryption for Windows IaaS VMs and back up and recover encrypted data.

In this module, you will:

- Describe Azure Disk Encryption.
- Configure Key Vault to support Azure Disk Encryption.
- Explain how to encrypt Azure IaaS VM hard disks.
- Back up and recover encrypted data from IaaS VM hard disks.

Lessons

- Introduction
- Describe Azure Disk Encryption and server-side encryption
- Configure Key Vault for Azure Disk Encryption
- Encrypt Azure IaaS Virtual Machine hard disks
- Back up and recover data from encrypted disks
- Create and encrypt a Windows Virtual Machine

Module 10: Implement change tracking and file integrity monitoring for Windows IaaS VMs

In this module, you'll learn how to monitor Windows Server Azure IaaS VMs for changes in files and the registry, as well as other monitor modifications made to application software.

In this module, you will:

- Implement Change Tracking and Inventory
- Manage Change Tracking and Inventory
- Manage tracked files
- Implement File Integrity Monitoring

- Select and monitor entities
- Use File Integrity Monitoring

Lessons

- Introduction
- Implement Change Tracking and Inventory
- Manage Change Tracking and Inventory
- Manage tracked files
- Implement File Integrity Monitoring
- Select and monitor entities
- Use File Integrity Monitoring

Module 11: Introduction to Cluster Shared Volumes

Learn about the core functionality, benefits, use cases, and implementation of Cluster Shared Volumes (CSV) in Windows Server 2019.

In this module, you will:

- Describe the functionality of CSV.
- Describe the architecture and components of CSV.
- Implement CSV.

Lessons

- Introduction
- Determine the functionality of Cluster Shared Volumes
- Explore the architecture and components of Cluster Shared Volumes
- Implement Cluster Shared Volumes

Module 12: Implement Windows Server failover clustering

Learn about the core functionality of Windows Server failover clustering, various configuration options for failover clustering, and the use of cluster sets.

In this module, you will:

- Describe Windows Server failover clustering.
- Implement Windows Server failover clustering.
- Manage Windows Server failover clustering.
- Implement stretch clusters.
- Describe cluster sets.

Lessons

- Introduction
- Define Windows Server failover clustering
- Plan Windows Server failover clustering
- Implement Windows Server failover clustering
- Manage Windows Server failover clustering
- Implement stretch clusters
- Define cluster sets

Module 13: Implement high availability of Windows Server VMs

Learn about the core functionality, benefits, use cases, and implementation of highly available Microsoft Hyper-V virtual machines (VMs) in Windows Server 2019.

In this module, you will:

- Describe cluster sets.
- Describe the Hyper-V high availability options.
- Describe Hyper-V VMs load balancing.
- Implement Hyper-V VMs live migration.
- Implement Hyper-V VMs storage migration.

Lessons

- Introduction
- Select high-availability options for Hyper-V
- Consider network load balancing for Hyper-V VMs
- Implement Hyper-V VM live migration
- Implement Hyper-V VMs storage migration

Module 14: Implement Windows Server File Server high availability

Learn about the core functionality, benefits, use cases, and implementation of the highly available File Server role in Windows Server 2019.

In this module, you will:

- Provide a high-level overview of Windows Server File Server high-availability options.
- Describe the characteristics of, and high-level implementation steps for Cluster Shared Volumes (CSV).
- Describe the characteristics of, and high-level implementation steps for Scale-Out File Server (SOFS).
- Describe the characteristics of, and high-level implementation steps for Storage Replica.

Lessons

- Introduction
- Explore the Windows Server File Server high-availability options
- Define Cluster Shared Volumes
- Implement Scale-Out File Server
- Implement Storage Replica

Module 15: Implement scale and high availability with Windows Server VM

You'll learn how to implement scaling for virtual machine scale sets and load-balanced VMs. You'll also learn how to implement Azure Site Recovery.

In this module, you will:

- Describe virtual machine scale sets.
- Implement scaling.
- Implement load-balancing virtual machines.
- Implement Azure Site Recovery.

Lessons

- Introduction
- Describe virtual machine scale sets
- Implement scaling
- Implement load-balancing VMs
- Create a virtual machine scale set in the Azure portal
- Describe Azure Site Recovery
- Implement Azure Site Recovery

Module 16: Implement Hyper-V Replica

Learn about Hyper-V Replica, scenarios for its use, and prerequisites to use it. Learn about Azure Site Recovery and the benefits of using it, focusing on implementing Site Recovery in on-premises scenarios.

In this module, you will:

- Describe Hyper-V Replica, pre-requisites for its use, and its high-level architecture and components.
- Describe Hyper-V Replica usage scenarios, available replication settings, and security considerations.
- Configure Hyper-V Replica settings, health monitoring, and failover options.
- Implement Hyper-V Replica.
- Describe extended replication.
- Describe Site Recovery.
- Implement Site Recovery.

Lessons

- Introduction
- Define Hyper-V Replica
- Plan for Hyper-V Replica
- Configure and implement Hyper-V Replica
- Define extended replication
- Define Azure Site Recovery
- Implement Site Recovery from on-premises site to Azure
- Implement Site Recovery from on-premises site to on-premises site

Module 17: Protect your on-premises infrastructure from disasters with Azure Site Recovery

Provide disaster recovery for your on-premises infrastructure by managing and orchestrating replication, failover, and failback of VMware virtual machines, Hyper-V virtual machines, and physical servers with Azure Site Recovery.

In this module, you will:

- Identify the features and protection capabilities Azure Site Recovery provides to on-premises infrastructure
- Identify the requirements for enabling protection of on-premises infrastructure

Lessons

- Introduction
- Azure Site Recovery overview
- Workloads supported for protection with Azure Site Recovery
- Run a disaster recovery drill
- Failover and failback

Module 18: Implement hybrid backup and recovery with Windows Server IaaS

You'll learn about Azure Backup before learning to implement Recovery Vaults and Azure Backup Policies. You'll learn to implement Windows IaaS VM recovery, perform backup and restore of on-premises workloads, and manage Azure VM backups.

In this module, you will:

- Describe Azure Backup.
- Implement Recovery Vaults.
- Implement Azure Backup policies.
- Recover Windows IaaS VMs.
- Perform file and folder recovery.
- Perform backup and recovery of on-premises workloads.
- Explain how to manage Azure VM backups with Azure Backup.

Lessons

- Introduction
- Describe Azure Backup
- Implement recovery vaults
- Implement Azure Backup policies
- Recover Windows IaaS Virtual Machines
- Perform file and folder recovery
- Perform backup and restore of on-premises workloads
- Manage Azure Virtual Machine backups with Azure Backup service

Module 19: Protect your Azure infrastructure with Azure Site Recovery

Provide disaster recovery for your Azure infrastructure by customizing replication, failover, and failback of Azure virtual machines with Azure Site Recovery.

In this module, you will:

- Protect Azure virtual machines with Azure Site Recovery

- Run a disaster recovery drill to validate protection
- Failover and failback your virtual machines

Lessons

- Introduction
- What is Azure Site Recovery
- Prepare for disaster recovery with Azure Site Recovery
- Exercise - Set up disaster recovery with Azure Site Recoveryv
- Run a disaster recovery drill
- Exercise - Run a disaster recovery drill
- Failover and failback using Azure Site Recovery
- Exercise - Failover and failback using Azure Site Recovery

Module 20: Protect your virtual machines by using Azure Backup

Use Azure Backup to help protect the data for on-premises servers, virtual machines, virtualized workloads such as SQL Server or SAP HANA running in Azure VMs, Azure file shares, and more.

In this module, you will:

- Identify the scenarios for which Azure Backup provides backup and restore capabilities
- Back up and restore an Azure virtual machine

Lessons

- Introduction
- Azure Backup features and scenarios
- Back up an Azure virtual machine by using Azure Backup
- Exercise - Back up an Azure virtual machine
- Restore virtual machine data
- Exercise - Restore Azure virtual machine data

Module 21: Active Directory Domain Services migration

Determine the best approach to moving domain controllers to Windows Server 2022. Learn how the Active Directory Migration Tool can consolidate domains within a forest or migrate domains to a new AD DS forest.

In this module, you will:

- Compare upgrading an AD DS forest and migrating to a new AD DS forest
- Describe how to upgrade an existing AD DS forest
- Describe how to migrate to a new AD DS forest
- Describe Active Directory Migration Tool (ADMT)

Lessons

- Introduction
- Examine upgrade vs. migration
- Upgrade a previous version of Active Directory Domain Services to Windows Server 2022
- Migrate to Active Directory Domain Services in Windows Server 2022 from a previous version
- Explore the Active Directory Migration Tool

Module 22: Migrate file server workloads using Storage Migration Service

Learn to use Storage Migration Service to migrate files and files shares from existing file server to new servers running Windows Server 2022. Configure storage migration for optimum performance of data migration.

In this module, you will:

- Describe Storage Migration Service and its usage scenarios
- Identify the requirements for using Storage Migration Service
- Describe how to migrate a server with storage migration
- List the considerations for using Storage Migration Service

Lessons

- Introduction
- Storage Migration Service overview and usage scenarios
- Storage migration requirements
- Migrate a server with Storage migration
- Evaluate storage migration considerations

Module 23: Migrate Windows Server roles

Learn how to install and use the Windows Server Migration Tools cmdlets to migrate commonly used server roles from earlier versions of Windows Server.

In this module, you will:

- Describe the Windows Server Migration Tools
- Use the migration tools to migrate specific Windows Server roles

Lessons

- Introduction
- Describe the Windows Server Migration Tools
- Install the Migration Tools
- Migrate roles using the Migration Tools

Module 24: Migrate on-premises Windows Server instances to Azure IaaS virtual machines

You'll be able to plan a migration and select appropriate server migration tools. You will also learn how to use Azure Migrate, how to assess physical servers, and how to migrate those servers.

In this module, you will:

- Plan your migration.
- Describe Azure Migrate.
- Migrate server workloads using Windows Server Migration Tools.
- Assess physical servers with Azure Migrate.
- Migrate on-premises servers to Azure.

Lessons

- Introduction
- Plan your migration
- Describe Azure Migrate
- Perform server assessment
- Assess physical servers with Azure Migrate
- Migrate Windows Server workloads by using Azure Migrate

Module 25: Upgrade and migrate Windows Server IaaS virtual machines

Learn to migrate a workload running in Windows Server to an infrastructure as a service (IaaS) virtual machine (VM) and to Windows Server 2019 by using Windows Server migration tools or the Storage Migration Service.

In this module, you will:

- Describe Windows Server IaaS migration.
- Explain how to migrate workloads using Windows Server Migration tools.
- Describe storage migration.
- Migrate file servers by using the Storage Migration Service.

Lessons

- Introduction
- Describe Azure Migrate
- Migrate Windows Server workloads by using Azure Migrate
- Describe storage migration
- Migrate file servers by using Storage Migration Service

Module 26: Containerize and migrate ASP.NET applications to Azure App Service
In this module, you'll learn to use the Azure Migrate App Containerization tool to containerize and migrate ASP.NET applications to Azure App Service.

In this module, you will:

- Discover and containerize your ASP.NET app running on Windows machines using Azure Migrate: App Containerization.
- Build a container image for your ASP.NET application.
- Deploy your containerized application to Azure App Service using Azure Migrate: App Containerization.

Lessons

- Introduction
- Azure Migrate App Containerization overview
- Exercise - Set up host environment
- Exercise - Discover your ASP.NET web application
- Exercise - Build container image for your ASP.NET app
- Exercise - Deploy app container to App Service

Module 27: Monitor Windows Server performance
Learn to use a range of Windows Server tools to monitor the operating system and applications on a server computer. You'll also learn to configure your system to optimize efficiency and to troubleshoot problems.

In this module, you will:

- Use built-in tools in Windows Server to monitor server performance
- Understand the fundamentals of server performance tuning

Lessons

- Introduction
- Use Performance Monitor to identify performance problems
- Use Resource Monitor to review current resource usage
- Review reliability with Reliability Monitor
- Implement a performance monitoring methodology
- Use Data Collector Sets to analyze server performance
- Monitor network infrastructure services
- Monitor virtual machines running Windows Server
- Monitor performance with Windows Admin Center
- Use System Insights to help predict future capacity issues
- Optimize the performance of Windows Server

Module 28: Manage and monitor Windows Server event logs

Learn how Event Viewer provides a convenient and accessible location for you to observe events that occur. Access event information quickly and conveniently. Learn how to interpret the data in the event log.

In this module, you will:

- Describe event logs
- Use Server Manager and Windows Admin Center to - Review event logs
- Implement custom views
- Configure an event subscription

Lessons

- Introduction
- Describe Windows Server event logs
- Use Windows Admin Center to review logs
- Use Server Manager to review logs
- Use custom views

- Implement event log subscriptions

Module 29: Implement Windows Server auditing and diagnostics

Learn to audit and diagnose your Windows Server environment for regulatory compliance, user activity, and troubleshooting. Implement security best practices through regular audits of your network environment to gain early warning of potential malicious activity.

In this module, you will:
- Audit Windows Server events
- Configure Windows Server to record diagnostic information

Lessons
- Introduction
- Describe basic auditing categories
- Describe advanced categories
- Log user access
- Enable setup and boot event collection

Module 30: Troubleshoot Active Directory

Learn how to troubleshoot AD DS service failures or degraded performance. Learn how to recover deleted security objects and the AD DS database, and how to troubleshoot hybrid authentication issues.

In this module, you will:
- Recover the AD DS database, objects in AD DS, and SYSVOL
- Troubleshoot AD DS replication
- Troubleshoot Hybrid authentication issues

Lessons
- Introduction
- Recover objects from the AD recycle bin
- Recover the AD DS database
- Recover SYSVOL
- Troubleshoot AD DS replication
- Troubleshoot hybrid authentication issues

Module 31: Monitor Windows Server IaaS Virtual Machines and hybrid instances

You'll be able to implement Azure Monitor for IaaS VMs in Azure, implement Azure Monitor in on-premises environments, and use dependency maps.

In this module, you will:
- Enable Azure Monitor for VMs.
- Monitor an Azure VM with Azure Monitor.
- Enable Azure Monitor in hybrid scenarios.
- Collect data from a Windows computer in a hybrid environment.
- Integrate Azure Monitor with Microsoft Operations Manager.

Lessons
- Introduction
- Enable Azure Monitor for Virtual Machines
- Monitor an Azure Virtual Machine with Azure Monitor
- Enable Azure Monitor in hybrid scenarios
- Collect data from a Windows computer in a hybrid environment
- Integrate Azure Monitor with Microsoft Operations Manager

Module 32: Monitor the health of your Azure virtual machine by using Azure Metrics Explorer and metric alerts

Evaluate monitoring options for an Azure virtual machine (VM). Enable diagnostics to get data about your VM. View VM metrics in Azure Metrics Explorer. Create a metric alert to monitor performance.

In this module, you will:

- Identify metrics and diagnostic data that you can collect for virtual machines
- Configure monitoring for a virtual machine
- Use monitoring data to diagnose problems

Lessons

- Introduction
- Monitor the health of the virtual machine
- Exercise - Set up a VM with boot diagnostics
- View VM metrics
- Configure the Azure Diagnostics extension
- Exercise - Configure the Azure Diagnostics extension
- Diagnostic data case studies

Module 33: Monitor performance of virtual machines by using Azure Monitor VM Insights

Deploy monitoring for workloads on virtual machines. Set up a log analytics workspace, onboard virtual machines to Azure Monitor VM Insights, and build log queries by using Kusto Query Language.

In this module, you will:

- Evaluate Azure Monitor Logs and Azure Monitor VM Insights.
- Configure a Log Analytics workspace.
- Build queries from the Heartbeat and InsightsMetrics tables.

Lessons

- Introduction
- What are Azure Monitor Logs and Azure Monitor VM Insights?
- Exercise - Set up a Log Analytics workspace and Azure Monitor VM Insights
- Build log queries by using the Kusto Query Language
- Exercise - Build log queries

Module 34: Insights Troubleshoot on-premises and hybrid networking

Learn to troubleshoot on-premises connectivity and hybrid network connectivity. Diagnose common issues with DHCP, name resolution, IP configuration, and routing that can cause reliability and connectivity problems in an on-premises and a hybrid environment.

In this module, you will:

- Diagnose DHCP and DNS problems in on-premises contexts
- Diagnose IP configuration and routing problems
- Implement Packet Monitor to help diagnose network problems
- Use Azure Network Watcher to troubleshoot Microsoft Azure virtual networks

Lessons

- Introduction
- Diagnose DHCP problems
- Diagnose DNS problems
- Diagnose IP configuration issues
- Diagnose routing problems
- Use Packet Manager to help diagnose network problems
- Use Azure Network Watcher to help diagnose network problems

Module 35: Troubleshoot Windows Server Virtual Machines in Azure

Learn to troubleshoot configuration issues that impact connectivity to your Azure-hosted Windows Server virtual machines (VMs). Explore approaches to resolve issues with VM startup, extensions, performance, storage, and encryption.

In this module, you will:

- Troubleshoot VM deployment and extension issues
- Troubleshoot VM startup and performance issues
- Troubleshoot VM storage and encryption issues
- Troubleshoot connectivity to VMs

Lessons

- Introduction
- Troubleshoot VM deployment
- Troubleshoot VM startup
- Troubleshoot VM extensions
- Troubleshoot VM connectivity
- Troubleshoot VM performance
- Troubleshoot VM storage

