

AZ-801: Configuring Windows Server Hybrid Advanced Services

Course details

Module 1: Secure Windows Server user accounts

- 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

Module 2: Hardening Windows Server

- 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

Module 3: Windows Server update management

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

Module 4: Secure Windows Server DNS

- 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.

Module 5: Implement Windows Server IaaS VM network security

- 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.

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

- 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.

Module 7: Manage Azure updates

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

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

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

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

- 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.

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

- 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

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

Module 12: Implement Windows Server failover clustering

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

Module 13: Implement high availability of Windows Server VMs

- 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.

Module 14: Implement Windows Server File Server high availability

- 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.

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

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

Module 16: Implement Hyper-V Replica

- 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.

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

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

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

- 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.

Module 19: Protect your Azure infrastructure with Azure Site Recovery

- Protect Azure virtual machines with Azure Site Recovery.
- Run a disaster recovery drill to validate protection.
- Failover and failback your virtual machines.

Module 20: Protect your virtual machines by using Azure Backup

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

Module 21: Active Directory Domain Services migration

- 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)

Module 22: Migrate file server workloads using Storage Migration Service

- 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

Module 23: Migrate Windows Server roles

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

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

- 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.

Module 25: Upgrade and migrate Windows Server IaaS virtual machines

- 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.

Module 26: Containerize and migrate ASP.NET applications to Azure App Service

- 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.

Module 27: Monitor Windows Server performance

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

Module 28: Manage and monitor Windows Server event logs

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

Module 29: Implement Windows Server auditing and diagnostics

- Audit Windows Server events
- Configure Windows Server to record diagnostic information

Module 30: Troubleshoot Active Directory

- Recover the AD DS database, objects in AD DS, and SYSVOL
- Troubleshoot AD DS replication
- Troubleshoot Hybrid authentication issues

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

- 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.

Module 32: Monitor your Azure virtual machines with Azure Monitor

- Understand which monitoring data you need to collect from your VM.
- Enable and view recommended alerts and diagnostics.
- Use Azure Monitor to collect and analyze VM host metrics data.
- Use Azure Monitor Agent to collect VM client performance metrics and event logs

Module 33: Troubleshoot on-premises and hybrid networking

- 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

Module 34: Troubleshoot Windows Server Virtual Machines in Azure

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