AZ-801T00: Configuring Windows Server Hybrid Advanced Services

Course Code: AZ-801T00
Duration: 4 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

This four-day instructor-led course is designed for IT professionals who configure advanced Windows Server services using on-premises, hybrid, and cloud technologies. These professionals manage and support an infrastructure that includes on-premises and Azure IaaS-hosted Windows Server-based workloads. 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 manage and secure Azure VMs running Windows Server. The course also covers how to perform tasks related to high availability, troubleshooting, and disaster recovery. The course highlights various 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.

SKILLS COVERED

- Harden the security configuration of the Windows Server operating system environment.
- Enhance hybrid security using Azure Security Center, Azure Sentinel, and Windows Update Management.
- Apply security features to protect critical resources.
- Implement high availability and disaster recovery solutions.
- Implement recovery services in hybrid scenarios.
- Plan and implement hybrid and cloud-only migration, backup, and recovery scenarios.
- Perform upgrades and migration related to AD DS, and storage.
- Manage and monitor hybrid scenarios using WAC, Azure Arc, Azure Automation and Azure Monitor.
- Implement service monitoring and performance monitoring, and apply troubleshooting.

WHO SHOULD ATTEND?

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.

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 management tools (implied in the first prerequisite).
- Basic knowledge of core Microsoft compute, storage, networking, and virtualization technologies (implied in the first prerequisite).

- 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

An understanding of the following concepts as related to Windows Server technologies:

- High availability and disaster recovery
- Automation
- Monitoring
- Troubleshooting

COURSE CONTENTS

Module 1: Windows Server security

This module discusses how to protect an Active Directory environment by securing user accounts to least privilege and placing them in the Protected Users group. The module covers how to limit authentication scope and remediate potentially insecure accounts. The module also describes how to harden the security configuration of a Windows Server operating system environment. In addition, the module discusses the use of Windows Server Update Services to deploy operating system updates to computers on the network. Finally, the module covers how to secure Windows Server DNS to help protect the network name resolution infrastructure.

Lessons

- Secure Windows Sever user accounts
- Hardening Windows Server
- Windows Server Update Management
- Secure Windows Server DNS

Lab : Configuring security in Windows Server

- Configuring Windows Defender Credential Guard
- Locating problematic accounts
- Implementing LAPS

After completing this module, students will be able to:

- Diagnose and remediate potential security vulnerabilities in Windows Server resources.
- Harden the security configuration of the Windows Server operating system environment.
- Deploy operating system updates to computers on a network by using Windows Server Update Services.
- Secure Windows Server DNS to help protect the network name resolution infrastructure.
- Implement DNS policies.

Module 2: Implementing security solutions in hybrid scenarios

This module describes how to secure on-premises Windows Server resources and Azure IaaS workloads. The module covers 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 addition, the module introduces Azure Security Center and explains how to onboard Windows Server computers to Security Center. The module also describes how to enable Azure Update Management, deploy updates, review an update assessment, and manage updates for Azure VMs. The modules explains how Adaptive application controls and BitLocker disk encryption are used to protect Windows Server IaaS VMs. Finally, the module explains how to monitor Windows Server Azure IaaS VMs for changes in files and the registry, as well as monitoring modifications made to application software.

Lessons

- Implement Windows Server IaaS VM network security.
- Audit the security of Windows Server IaaS Virtual Machines
- Manage Azure updates
- Create and implement application allowlists with adaptive application control
- Configure BitLocker disk encryption for Windows IaaS Virtual Machines
- Implement change tracking and file integrity monitoring for Windows Server IaaS VMs

Lab : Using Azure Security Center in hybrid scenarios

- Provisioning Azure VMs running Windows Server
- Configuring Azure Security Center
- Onboarding on-premises Windows Server into Azure Security Center
- Verifying the hybrid capabilities of Azure Security Center
- Configuring Windows Server 2019 security in Azure VMs

After completing this module, students will be able to:

- Diagnose network security issues in Windows Server IaaS virtual machines.
- Onboard Windows Server computers to Azure Security Center.
- Deploy and manage updates for Azure VMs by enabling Azure Automation Update Management.
- Implement Adaptive application controls to protect Windows Server IaaS VMs.
- Configure Azure Disk Encryption for Windows IaaS virtual machines (VMs).
- Back up and recover encrypted data.
- Monitor Windows Server Azure IaaS VMs for changes in files and the registry.

Module 3: Implementing high availability

This module describes technologies and options to create a highly available Windows Server environment. The module introduces Clustered Shared Volumes for shared storage access across multiple cluster nodes. The module also highlights failover clustering, stretch clusters, and cluster sets for implementing high availability of Windows Server workloads. The module then discusses high availability provisions for Hyper-V and Windows Server VMs, such as network load balancing, live migration, and storage migration. The module also covers high availability options for shares hosted on Windows Server file servers. Finally, the module describes how to implement scaling for virtual machine scale sets and load-balanced VMs, and how to implement Azure Site Recovery.

Lessons

- Introduction to Cluster Shared Volumes.
- Implement Windows Server failover clustering.
- Implement high availability of Windows Server VMs.
- Implement Windows Server File Server high availability.
- Implement scale and high availability with Windows Server VMs.

Lab : Implementing failover clustering

- Configuring iSCSI storage
- Configuring a failover cluster
- Deploying and configuring a highly available file server
- Validating the deployment of the highly available file server

After completing this module, students will be able to:

- Implement highly available storage volumes by using Clustered Share Volumes.
- Implement highly available Windows Server workloads using failover clustering.
- Describe Hyper-V VMs load balancing.
- Implement Hyper-V VMs live migration and Hyper-V VMs storage migration.
- Describe Windows Server File Server high availablity options.
- Implement scaling for virtual machine scale sets and load-balanced VMs.
- Implement Azure Site Recovery.

Module 4: Disaster recovery in Windows Server

This module introduces Hyper-V Replica as a business continuity and disaster recovery solution for a virtual environment. The module discusses Hyper-V Replica scenarios and use cases, and prerequisites to use it. The module also discusses how to implement Azure Site Recovery in on-premises scenarios to recover from disasters.

Lessons

- Implement Hyper-V Replica
- Protect your on-premises infrastructure from disasters with Azure Site Recovery

Lab : Implementing Hyper-V Replica and Windows Server Backup

- Implementing Hyper-V Replica
- Implementing backup and restore with Windows Server Backup

After completing this module, students will be able to:

- Describe Hyper-V Replica, pre-requisites for its use, and its high-level architecture and components
- Describe Hyper-V Replica use cases and security considerations.
- Configure Hyper-V Replica settings, health monitoring, and failover options.
- Describe extended replication.
- Replicate, failover, and failback virtual machines and physical servers with Azure Site Recovery.

Module 5: Implementing recovery services in hybrid scenarios

This module covers tools and technologies for implementing disaster recovery in hybrid scenarios, whereas the previous module focus on BCDR solutions for on-premises scenarios. The module begins with Azure Backup as a service to protect files and folders before highlighting how to implementRecovery Vaults and Azure Backup Policies. The module describes how to recover Windows IaaS virtual machines,

perform backup and restore of on-premises workloads, and manage Azure VM backups. The modules also covers how to provide disaster recovery for Azure infrastructure by managing and orchestrating replication, failover, and failback of Azure virtual machines with Azure Site Recovery.

Lessons

- Implement hybrid backup and recovery with Windows Server IaaS
- Protect your Azure infrastructure with Azure Site Recovery
- Protect your virtual machines by using Azure Backup

Lab : Implementing Azure-based recovery services

- Implementing the lab environment
- Creating and configuring an Azure Site Recovery vault
- Implementing Hyper-V VM protection by using Azure Site Recovery vault
- Implementing Azure Backup

After completing this module, students will be able to:

- Recover Windows Server IaaS virtual machines by using Azure Backup.
- Use Azure Backup to help protect the data for on-premises servers and virtualized workloads.
- Implement Recovery Vaults and Azure Backup policies.
- Protect Azure VMs with Azure Site Recovery.
- Run a disaster recovery drill to validate protection.
- Failover and failback Azure virtual machines.

Module 6: Upgrade and migrate in Windows Server

This module discusses approaches to migrating Windows Server workloads running in earlier versions of Windows Server to more current versions. The module covers the necessary strategies needed to move domain controllers to Windows Server 2022 and describes how the Active Directory Migration Tool can consolidate domains within a forest or migrate domains to a new AD DS forest. The module also discusses the use of Storage Migration Service to migrate files and files shares from existing file servers to new servers running Windows Server 2022. Finally, the module covers how to install and use the Windows Server Migration Tools cmdlets to migrate commonly used server roles from earlier versions of Windows Server.

Lessons

- Active Directory Domain Services migration
- Migrate file server workloads using Storage Migration Service
- Migrate Windows Server roles

Lab : Migrating Windows Server workloads to IaaS VMs

- Deploying AD DS domain controllers in Azure
- Migrating file server shares by using Storage Migration Service

After completing this module, students will be able to:

- Compare upgrading an AD DS forest and migrating to a new AD DS forest.
- Describe the Active Directory Migration Tool (ADMT).
- Identify the requirements and considerations for using Storage Migration Service.

- Describe how to migrate a server with storage migration.
- Use the Windows Server Migration Tools to migrate specific Windows Server roles.

Module 7: Implementing migration in hybrid scenarios

After completing this module, students will be able to:

- Plan a migration strategy and choose the appropriate migration tools.
- Perform server assessment and discovery using Azure Migrate.
- Migrate Windows Server workloads to Azure VM workloads using Azure Migrate.
- Explain how to migrate workloads using Windows Server Migration tools.
- Migrate file servers by using the Storage Migration Service.
- Discover and containerize ASP.NET applcations running on Windows.
- Migrate a containerized application to Azure App Service.

Module 8: Server and performance monitoring in Windows Server

This module introduces a range of tools to monitor the operating system and applications on a Windows Server computer as well as describing how to configure a system to optimize efficiency and to troublshoot problems. The module covers how Event Viewer provides a convenient and accessible location for observing events that occur, and how to interpret the data in the event log. The module also covers how to audit and diagnose a Windows Server environment for regulatory compliance, user activity, and troubleshooting. Finally, the module explains how to troubleshoot AD DS service failures or degraded performance, including recovery of deleted objects and the AD DS database, and how to troubleshoot hybrid authentication issues.

Lessons

- Monitor Windows Server performance
- Manage and monitor Windows Server event logs
- Implement Windows Server auditing and diagnostics
- Troubleshoot Active Directory

Lab : Monitoring and troubleshooting Windows Server

- Establishing a performance baseline
- Identifying the source of a performance problem
- Viewing and configuring centralized event logs

After completing this module, students will be able to:

- Explain the fundamentals of server performance tuning.
- Use built-in tools in Windows Server to monitor server performance.
- Use Server Manager and Windows Admin Center to review event logs.
- Implement custom views.
- Configure an event subscription.
- Audit Windows Server events.
- Configure Windows Server to record diagnostic information.
- Recover the AD DS database and objects in AD DS.
- Troubleshoot AD DS replication.
- Troubleshoot hybrid authentication issues.

Module 9: Implementing operational monitoring in hybrid scenarios

This module covers using monitoring and troubleshooing tools, processes, and best

practices to streamline app performance and availabilty of Windows Server IaaS VMs and hybrid instances. The module describes how to implement Azure Monitor for IaaS VMs in Azure, implement Azure Monitor in on-premises environments, and use dependency maps. The module then explains how to enable diagnostics to get data about a VM, and how to view VM metrics in Azure Metrics Explorer, and how to create a metric alert to monitor VM performance. The module then covers how to monitor VM performance by using Azure Monitor VM Insights. The module then describes various aspects of troubleshooting on premises and hybrid network connectivity, including how to diagnose common issues with DHCP, name resolution, IP configuration, and routing. Finally, the module examines how to troubleshoot configuration issues that impact connectivity to Azure-hosted Windows Server virtual machines (VMs), as well as approaches to resolve issues with VM startup, extensions, performance, storage, and encryption.

Lessons

- Monitor Windows Server IaaS Virtual Machines and hybrid instances
- Monitor the health of your Azure virtual machines by using Azure Metrics Explorer and metric alerts
- Monitor performance of virtual machines by using Azure Monitor VM Insights
- Troubleshoot on-premises and hybrid networking
- Troubleshoot Windows Server Virtual Machines in Azure

Lab : Monitoring and troubleshooting of IaaS VMs running Windows Server

- Enabling Azure Monitor for virtual machines
- Setting up a VM with boot diagnostics
- Setting up a Log Analytics workspace and Azure Monitor VM Insights

After completing this module, students will be able to:

- Implement Azure Monitor for IaaS VMs in Azure and in on-premises environments.
- Implement Azure Monitor for IaaS VMs in Azure and in on-premises environments.
- View VM metrics in Azure Metrics Explorer.
- Use monitoring data to diagnose problems.
- Evaluate Azure Monitor Logs and configure Azure Monitor VM Insights.
- Configure a Log Analytics workspace.
- Troubleshoot on-premises connectivity and hybrid network connectivity.
- Troubleshoot AD DS service failures or degraded performance.
- Recover deleted security objects and the AD DS database.
- Troubleshoot hybrid authentication issues.

END OF PAGE