AZ-801T00: Configuring Windows Server Hybrid Advanced Services

Duration: 32 Hours (4 Days)

Course Overview

The AZ-801T00: Configuring Windows Server Hybrid Advanced Services course is designed for IT professionals who seek to enhance their skills in implementing, managing, and maintaining a Windows Server hybrid environment. This course covers various advanced topics, including Securing Windows Server infrastructures, Implementing high availability, disaster recovery, Server migration, and Monitoring/troubleshooting. In Module 1, learners focus on securing both on-premises and hybrid infrastructures, emphasizing Operating system security, Active Directory, network, and Storage security, as well as using Azure services to identify and remediate security issues. Module 2 delves into high availability through Failover clustering and Managing Storage Spaces directly, while Module 3 centers on disaster recovery techniques, including Azure Site Recovery and Hyper-V replicas. Module 4 is vital for understanding Server and workload migrations, from on-premises to Azure and upgrading to Windows Server 2022. Lastly, Module 5 equips participants with the knowledge to monitor and troubleshoot diverse environments effectively, using both native Windows Server tools and Azure services. For IT professionals seeking to pass the Microsoft AZ-801 exam, this course is an essential step in acquiring the expertise necessary for optimizing and securing server environments.

Audience Profile

The AZ-801T00 course equips IT professionals with advanced Windows Server hybrid configuration and security skills.

- Target Audience Job Roles:
- Systems Administrators
- Windows Server Administrators
- IT Professionals with experience in Windows Server and Azure environments
- Network Engineers focusing on Windows Server infrastructure
- Security Specialists overseeing Windows Server and hybrid Active Directory
- Disaster Recovery Consultants
- Infrastructure Architects planning server migrations and high availability
- Cloud Solutions Architects with a focus on Microsoft Azure and Windows Server
- Technical Support Engineers for Windows Server environments
- IT Professionals looking to upgrade skills from older versions to Windows Server 2022
- IT Managers overseeing Windows Server infrastructure and cloud integration

Course Syllabus

Secure Windows Server on-premises and hybrid infrastructures (25– 30%)

Secure Windows Server operating system

- Configure and manage Exploit Protection
- Configure and manage Windows Defender Application Control
- Configure and manage Microsoft Defender for Servers

- Configure and manage Windows Defender Credential Guard
- Configure SmartScreen
- Implement operating system security by using Group Policies

Secure a hybrid Active Directory infrastructure

- Configure password policies
- Enable password block lists
- Manage protected users
- Manage account security on a Read-Only Domain Controller (RODC)
- Harden domain controllers
- Configure authentication policy silos
- Restrict access to domain controllers
- Configure account security
- Manage AD built-in administrative groups
- Manage AD delegation
- Implement and manage Microsoft Defender for Identity

Identify and remediate Windows Server security issues by using Azure services

- Monitor on-premises servers and Azure VMs by using Microsoft Sentinel
- Identify and remediate security issues in on-premises servers and Azure
- VMs by using Microsoft Defender for Cloud

Secure Windows Server networking

- Manage Windows Defender Firewall
- Implement domain isolation
- Implement connection security rules

Secure Windows Server storage

- Manage Windows BitLocker Drive Encryption (BitLocker)
- Manage and recover encrypted volumes
- Enable storage encryption by using Azure Disk Encryption
- Manage disk encryption keys for IaaS virtual machines

Implement and manage Windows Server high availability (10–15%)

Implement a Windows Server failover cluster

- Implement a failover cluster on-premises, hybrid, or cloud-only
- Create a Windows failover cluster
- Implement a stretch cluster across datacenters or Azure regions
- Configure storage for failover clustering
- Modify quorum options
- Configure network adapters for failover clustering
- Configure cluster workload options
- Configure cluster sets
- Configure Scale-Out File servers
- Create an Azure witness
- Configure a floating IP address for the cluster

- Implement load balancing for the failover cluster

Manage failover clustering

- Implement cluster-aware updating
- Recover a failed cluster node
- Upgrade a node to Windows Server 2022
- Failover workloads between nodes
- Install Windows updates on cluster nodes
- Manage failover clusters using Windows Admin Center

Implement and manage Storage Spaces Direct

- Create a failover cluster using Storage Spaces Direct
- Upgrade a Storage Spaces Direct node
- Implement networking for Storage Spaces Direct
- Configure Storage Spaces Direct

Implement disaster recovery (10–15%)

Manage backup and recovery for Windows Server

- Backup and restore files and folders to Azure Recovery Services Vault
- Install and manage Azure Backup Server
- Back up and recover using Azure Backup Server
- Manage backups in Azure Recovery Services Vault
- Create a backup policy
- Configure backup for Azure VM using the built-in backup agent
- Recover VM using temporary snapshots
- Recover VMs to new Azure VMs
- Restore a VM

Implement disaster recovery by using Azure Site Recovery

- Configure Azure Site Recovery networking
- Configure Site Recovery for on-premises VMs
- Configure a recovery plan
- Configure Site Recovery for Azure VMs
- Implement VM replication to secondary datacenter or Azure region
- Configure Azure Site Recovery policies

Protect virtual machines by using Hyper-V replicas

- Configure Hyper-V hosts for replication
- Manage Hyper-V replica servers
- Configure VM replication
- Perform a failover

Migrate servers and workloads (20–25%)

Migrate on-premises storage to on-premises servers or Azure

- Transfer data and share

- Cut over to a new server by using Storage Migration Service (SMS)
- Use Storage Migration Service to migrate to Azure VMs
- Migrate to Azure file shares

Migrate on-premises servers to Azure

- Deploy and configure Azure Migrate appliance
- Migrate VM workloads to Azure IaaS
- Migrate physical workloads to Azure IaaS
- Migrate by using Azure Migrate

Migrate workloads from previous versions to Windows Server 2022

- Migrate IIS
- Migrate Hyper-V hosts
- Migrate Remote Desktop Services (RDS) host servers
- Migrate Dynamic Host Configuration protocol (DHCP)
- Migrate print servers

Migrate IIS workloads to Azure

- Migrate IIS workloads to Azure Web Apps
- Migrate IIS workloads to containers

Migrate an Active Directory Domain Services (AD DS) infrastructure to Windows Server 2022 AD DS

- Migrate AD DS objects, including users, groups and Group Policies using
- AD Migration Tool
- Migrate to a new Active Directory Forest
- Upgrade an existing forest

Monitor and troubleshoot Windows Server environments (20–25%)

Monitor Windows Server by using Windows Server tools and Azure services

- Monitor Windows Server by using Performance Monitor
- Create and configure Data Collector Sets
- Monitor servers and configure alerts by using Windows Admin Center
- Analyze Windows Server system data by using System Insights
- Manage event logs
- Deploy Azure Monitor agents
- Collect performance counters to Azure
- Create alerts
- Monitor Azure VMs by using Azure diagnostics extension
- Monitor Azure VMs performance by using VM Insights

Troubleshoot Windows Server on-premises and hybrid networking

- Troubleshoot hybrid network connectivity
- Troubleshoot on-premises connectivity
- Troubleshoot Windows Server virtual machines in Azure
- Troubleshoot deployment failures

- Troubleshoot booting failures
- Troubleshoot VM performance issues
- Troubleshoot VM extension issues
- Troubleshoot disk encryption issues
- Troubleshoot storage
- Troubleshoot VM connection issues

Troubleshoot Active Directory

- Restore objects from AD recycle bin
- Recover Active Directory database using Directory Services Restore mode
- Recover system volume (SYSVOL)
- Troubleshoot Active Directory replication
- Troubleshoot Hybrid authentication issues
- Troubleshoot on-premises Active Director