Exam AZ-801: Configuring Windows Server Hybrid Advanced Services – Skills Measured

Audience Profile

Candidates for the Windows Server Hybrid Administrator Associate certification should have subject matter expertise in configuring and managing Windows Server on-premises, hybrid, and infrastructure as a service (IaaS) platform workloads.

Responsibilities for this role include integrating Windows Server environments with Azure services and managing Windows Server in on-premises networks. This role manages and maintains Windows Server IaaS workloads in Azure, in addition to migrating and deploying workloads to Azure.

This role typically collaborates with Azure administrators, enterprise architects, Microsoft 365 administrators, and network engineers.

Candidates for this exam configure advanced Windows Server services using on-premises, hybrid, and cloud technologies. These professionals should have expertise in implementing and managing on-premises and hybrid solutions, including performing tasks related to security, migration, monitoring, high availability, troubleshooting, and disaster recovery. They use administrative tools and technologies, such as Windows Admin Center, PowerShell, Azure Arc, Azure Automation Update Management, Microsoft Defender for Identity, Azure Security Center, Azure Migrate, and Azure Monitor.

A candidate for this exam should have extensive experience working with Windows Server operating systems.

Skills Measured

NOTE: The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. This list is NOT definitive or exhaustive.

NOTE: Most questions cover features that are general availability (GA). The exam may contain questions on Preview features if those features are commonly used.

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 Windows Defender for Endpoint
- configure and manage Windows Defender Credential Guard
- configure SmartScreen
- implement operating system security by using Group Policies

Secure a hybrid Active Directory (AD) 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 policies 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 IaaS virtual machines (VMs) by using Azure Sentinel
- identify and remediate security issues on-premises servers and Azure IaaS VMs by using Azure Security Center

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
- stretch cluster across datacenter 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

- back up 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 Virtual Machines using the built-in backup agent
- recover a VM using temporary snapshots
- recover VMs to new Azure Virtual Machines

- 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 Virtual Machines
- 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
- use Storage Migration Service to migrate to Azure Virtual Machines
- 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 Internet Information Services (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 AD DS infrastructure to Windows Server 2022 AD DS

- migrate AD DS objects, including users, groups and Group Policies, using Active Directory 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
- monitor by using System Insights
- manage event logs
- deploy Log Analytics agents
- collect performance counters to Azure
- create alerts
- monitor Azure Virtual Machines by using Azure diagnostics extension
- monitor Azure Virtual Machines 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 SYSVOL
- troubleshoot Active Directory replication
- troubleshoot hybrid authentication issues
- troubleshoot on-premises Active Directory