

Deploy and manage Active Directory Domain Services (AD DS) in on premises and cloud environments (30–35%)

Deploy and manage AD DS domain controllers

- deploy and manage domain controllers on-premises
- deploy and manage domain controllers in Azure
- deploy Read-Only Domain Controllers (RODCs)
- troubleshoot flexible single master operations (FSMO) roles

Configure and manage multi-site, multi-domain, and multi-forest environments

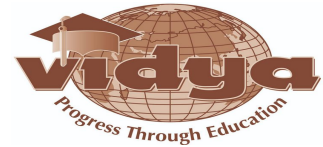
- configure and manage forest and domain trusts
- configure and manage AD DS sites
- configure and manage AD DS replication

Create and manage AD DS security principals

- create and manage AD DS users and groups
- manage users and groups in multi-domain and multi-forest scenarios
- implement group managed service accounts (gMSAs)
- join Windows Servers to AD DS, Azure AD DS, and Azure AD

Implement and manage hybrid identities

- implement Azure AD Connect
- manage Azure AD Connect Synchronization
- implement Azure AD Connect cloud sync
- integrate Azure AD, AD DS, and Azure AD DS
- manage Azure AD DS



- manage Azure AD Connect Health
- manage authentication in on-premises and hybrid environments
- configure and manage AD DS passwords

Manage Windows Server by using domain-based Group Policies

- implement Group Policy in AD DS
- implement Group Policy Preferences in AD DS
- implement Group Policy in Azure AD DS

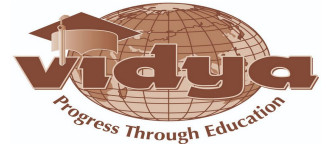
Manage Windows Servers and workloads in a hybrid environment (10– 15%)

Manage Windows Servers in a hybrid environment

- deploy a Windows Admin Center gateway server
- configure a target machine for Windows Admin Center
- configure PowerShell Remoting
- configure CredSSP or Kerberos delegation for second hop remoting
- configure JEA for PowerShell Remoting

Manage Windows Servers and workloads by using Azure services

- manage Windows Servers by using Azure Arc
- assign Azure Policy Guest Configuration
- deploy Azure services using Azure Virtual Machine extensions on non-Azure machines
- manage updates for Windows machines
- integrate Windows Servers with Log Analytics
- integrate Windows Servers with Azure Security Center
- manage IaaS virtual machines (VMs) in Azure that run Windows



- Server
- implement Azure Automation for hybrid workloads
 - create runbooks to automate tasks on target VMs
 - implement DSC to prevent configuration drift in IaaS machines

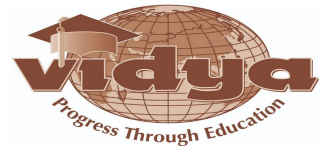
Manage virtual machines and containers (15–20%)

Manage Hyper-V and guest virtual machines

- enable VM enhanced session mode
- manage VM using PowerShell Remoting, PowerShell Direct, and HVC.exe
- configure nested virtualization
- configure VM memory
- configure Integration Services
- configure Discrete Device Assignment
- configure VM Resource Groups
- configure VM CPU Groups
- configure hypervisor scheduling types
- manage VM Checkpoints
- implement high availability for virtual machines
- manage VHD and VHDX files
- configure Hyper-V network adapter
- configure NIC teaming
- configure Hyper-V switch

Create and manage containers

- create Windows Server container images
- manage Windows Server container images
- configure Container networking



- manage container instances

Manage Azure Virtual Machines that run Windows Server

- manage data disks
- resize Azure Virtual Machines
- configure continuous delivery for Azure Virtual Machines
- configure connections to VMs
- manage Azure Virtual Machines network configuration

Implement and manage an on-premises and hybrid networking infrastructure (15–20%)

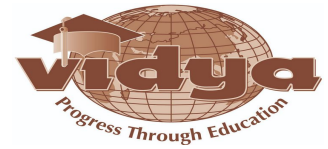
Implement on-premises and hybrid name resolution

- integrate DNS with AD DS
- create and manage zones and records
- configure DNS forwarding/conditional forwarding
- integrate Windows Server DNS with Azure DNS private zones
- implement DNSSEC

Manage IP addressing in on-premises and hybrid scenarios

- implement and manage IPAM
- implement and configure the DHCP server role (on-premises only)
- resolve IP address issues in hybrid environments
- create and manage scopes
- create and manage IP reservations
- implement DHCP high availability

Implement on-premises and hybrid network connectivity



- implement and manage the Remote Access role
- implement and manage Azure Network Adapter
- implement and manage Azure Extended Network
- implement and manage Network Policy Server role
- implement Web Application Proxy
- implement Azure Relay
- implement site-to-site virtual private network (VPN)
- implement Azure Virtual WAN
- implement Azure AD Application Proxy

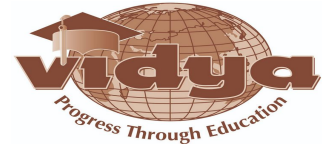
Manage storage and file services (15–20%)

Configure and manage Azure File Sync

- create Azure File Sync service
- create sync groups
- create cloud endpoints
- register servers
- create server endpoints
- configure cloud tiering
- monitor File Sync
- migrate DFS to Azure File Sync

Configure and manage Windows Server file shares

- configure Windows Server file share access
- configure file screens
- configure File Server Resource Manager (FSRM) quotas
- configure BranchCache



- implement and configure Distributed File System

(DFS) Configure Windows Server storage

- configure disks and volumes
- configure and manage Storage Spaces
- configure and manage Storage Replica
- configure Data Deduplication
- configure SMB direct
- configure Storage Quality of Service (QoS)
- configure file systems

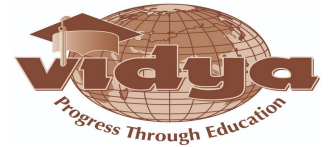
Secure Windows Server on-premises and hybrid infrastructures (25– 30%)

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

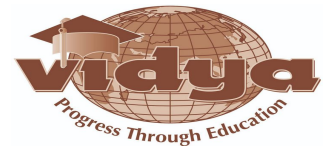
Secure Windows Server storage

- 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

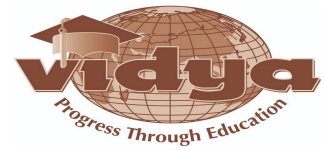
- implement cluster-aware updating
- recover a failed cluster node
- upgrade a node to Windows Server 2022
- failover workloads between nodes
- install Windows updates on cluster nodes
- manage failover clusters using Windows Admin Center

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