AZ-700T00: Designing and Implementing Microsoft Azure Networking Solutions

Duration: 24 Hours (3 Days)

Overview

The AZ-700T00: Designing and Implementing Microsoft Azure Networking Solutions course is an in-depth training program focused on Azure networking features and components. It is aimed at IT professionals who want to learn how to design, implement, and manage Azure networking solutions. Throughout the course, learners will explore various aspects of Azure networking, such as Virtual networks, Hybrid connections, ExpressRoute, Load balancing, network security, and Network monitoring.Starting with an understanding of Azure Virtual networks, Public and private DNS services, and Connectivity options, students will progress through hybrid networking design, including VPNs and Azure Virtual WAN. They will also delve into ExpressRoute for private connectivity, Load balancing for both HTTP(S) and non-HTTP(S) traffic using Azure services, and ensuring network security with tools like Azure Firewall and DDoS Protection.Modules on private access to Azure services will cover Azure Private Link and endpoints, while the Network monitoring section will teach students about monitoring network performance and health. By completing the course, learners will gain valuable skills in managing Azure networking components, preparing them for the AZ-700 certification exam and enhancing their career prospects in cloud networking.

Audience Profile

The AZ-700T00 course is designed for IT professionals looking to master Azure networking solutions for enhanced cloud infrastructure.

- Network Engineers and Architects involved in cloud solutions design
- Cloud Solutions Architects focusing on Azure infrastructure
- Azure Administrators managing virtual networks and hybrid connections
- IT Security Professionals responsible for network security
- DevOps Engineers integrating Azure networking into deployment pipelines
- Infrastructure Engineers transitioning from on-premises to cloud-based networks
- IT Professionals seeking certification in Azure networking services
- System Integrators implementing complex cloud networking solutions
- Technical Consultants providing advice on Azure networking best practices
- IT Project Managers overseeing cloud infrastructure projects

Course Syllabus

Skills at a glance

- Design and implement core networking infrastructure (25–30%)
- Design, implement, and manage connectivity services (20–25%)
- Design and implement application delivery services (15–20%)
- Design and implement private access to Azure services (10–15%)
- Design and implement Azure network security services (15–20%)
- Design and implement core networking infrastructure (25–30%)

Design and implement IP addressing for Azure resources

- Plan and implement network segmentation and address spaces
- Create a virtual network (VNet)
- Plan and configure subnetting for services, including VNet gateways,
- private endpoints, service endpoints, firewalls, application gateways,
- VNet-integrated platform services, and Azure Bastion
- Plan and configure subnet delegation
- Plan and configure shared or dedicated subnets
- Create a prefix for public IP addresses
- Choose when to use a public IP address prefix
- Plan and implement a custom public IP address prefix (bring your own IP)
- Create a public IP address
- Associate public IP addresses to resources
- Upgrade IP address SKU

Design and implement name resolution

- Design name resolution inside a VNet
- Configure DNS settings for a VNet
- Design public DNS zones
- Design private DNS zones
- Configure public and private DNS zones
- Link a private DNS zone to a VNet
- Design and implement Azure DNS Private Resolver

Design and implement VNet connectivity and routing

- Design service chaining, including gateway transit
- Implement VNet peering
- Implement and manage virtual networks by using Azure Virtual Network Manager
- Design and implement user-defined routes (UDRs)
- Associate a route table with a subnet
- Configure forced tunneling
- Diagnose and resolve routing issues
- Design and implement Azure Route Server
- Identify appropriate use cases for a network address translation (NAT) gateway
- Implement a NAT gateway

Monitor networks

- Configure monitoring, network diagnostics, and logs in Azure Network Watcher
- Monitor and troubleshoot network health by using Azure Network Watcher
- Monitor and troubleshoot networks by using Azure Monitor Network Insights
- Activate and monitor distributed denial-of-service (DDoS) protection
- Evaluate network security recommendations identified by Microsoft
- Defender for Cloud Secure Score
- Evaluate network security recommendations identified by Microsoft
- Defender For Cloud Attack Path Analysis
- Identify network resources by using Microsoft Defender for Cloud Security Explorer

- Design, implement, and manage connectivity services (20–25%)

Design, implement, and manage a site-to-site VPN connection

- Design a site-to-site VPN connection, including for high availability
- Select an appropriate VNet gateway stock-keeping unit (SKU) for site-tosite VPN requirements
- Implement a site-to-site VPN connection
- Identify when to use a policy-based VPN versus a route-based VPN connection
- Create and configure a local network gateway
- Create and configure an IPsec/Internet Key Exchange (IKE) policy
- Create and configure a virtual network gateway
- Diagnose and resolve virtual network gateway connectivity issues
- Implement Azure Extended Network

Design, implement, and manage a point-to-site VPN connection

- Select an appropriate virtual network gateway SKU for point-to-site VPN requirements
- Select and configure a tunnel type
- Select an appropriate authentication method
- Configure RADIUS authentication
- Configure authentication by using Microsoft Entra ID
- Implement a VPN client configuration file
- Diagnose and resolve client-side and authentication issues
- Specify Azure requirements for Always On VPN
- Specify Azure requirements for Azure Network Adapter

Design, implement, and manage Azure ExpressRoute

- Select an ExpressRoute connectivity model
- Select an appropriate ExpressRoute SKU and tier
- Design and implement ExpressRoute to meet requirements, including
- cross-region connectivity, redundancy, and disaster recovery
- Design and implement ExpressRoute options, including Global Reach,
- FastPath, and ExpressRoute Direct
- Choose between Azure private peering only, Microsoft peering only, or both
- Configure Azure private peering
- Configure Microsoft peering
- Create and configure an ExpressRoute gateway
- Connect a virtual network to an ExpressRoute circuit
- Recommend a route advertisement configuration
- Configure encryption over ExpressRoute
- Implement Bidirectional Forwarding Detection
- Diagnose and resolve ExpressRoute connection issues

Design and implement an Azure Virtual WAN architecture

- Select a Virtual WAN SKU
- Design a Virtual WAN architecture, including selecting types and services
- Create a hub in Virtual WAN
- Choose an appropriate scale unit for each gateway type
- Deploy a gateway into a Virtual WAN hub

- Configure virtual hub routing
- Integrate a Virtual WAN hub with a third-party NVA for cloud connectivity
- Design and implement application delivery services (15–20%)

Design and implement Azure Load Balancer and Azure Traffic Manager

- Map requirements to features and capabilities of Azure Load Balancer
- Identify appropriate use cases for Azure Load Balancer
- Choose an Azure Load Balancer SKU and tier
- Choose between public and internal load balancers
- Choose between regional and global load balancers
- Create and configure an Azure Load Balancer
- Implement Azure Traffic Manager
- Implement a gateway load balancer
- Implement a load balancing rule
- Create and configure inbound NAT rules
- Create and configure explicit outbound rules, including source network
- address translation (SNAT)

Design and implement Azure Application Gateway

- Map requirements to features and capabilities of Azure Application Gateway
- Identify appropriate use cases for Azure Application Gateway
- Choose between manual and autoscale
- Create a back-end pool
- Configure health probes
- Configure listeners
- Configure routing rules
- Configure HTTP settings
- Configure Transport Layer Security (TLS)
- Configure rewrite sets

Design and implement Azure Front Door

- Map requirements to features and capabilities of Azure Front Door
- Identify appropriate use cases for Azure Front Door
- Choose an appropriate tier
- Configure an Azure Front Door, including routing, origins, and endpoints
- Configure SSL termination and end-to-end SSL encryption
- Configure caching
- Configure traffic acceleration
- Implement rules, URL rewrite, and URL redirect
- Secure an origin by using Azure Private Link in Azure Front Door
- Design and implement private access to Azure services (10–15%)

Design and implement Azure Private Link service and Azure private endpoints

- Plan private endpoints
- Create private endpoints
- Configure access to private endpoints

- Create a Private Link service
- Integrate Private Link and Private Endpoint with DNS
- Integrate a Private Link service with on-premises clients

Design and implement service endpoints

- Choose when to use a service endpoint
- Create service endpoints
- Configure service endpoint policies
- Configure access to service endpoints
- Design and implement Azure network security services (15–20%)

Implement and manage network security groups

- Create a network security group (NSG)
- Associate a NSG to a resource
- Create an application security group (ASG)
- Associate an ASG to a network interface card (NIC)
- Create and configure NSG rules
- Interpret NSG flow logs
- Validate NSG flow rules
- Verify IP flow
- Configure an NSG for remote server administration, including Azure Bastion

Design and implement Azure Firewall and Azure Firewall Manager

- Map requirements to features and capabilities of Azure Firewall
- Select an appropriate Azure Firewall SKU
- Design an Azure Firewall deployment
- Create and implement an Azure Firewall deployment
- Configure Azure Firewall rules
- Create and implement Azure Firewall Manager policies
- Create a secure hub by deploying Azure Firewall inside an Azure Virtual WAN hub

Design and implement a Web Application Firewall (WAF) deployment

- Map requirements to features and capabilities of WAF
- Design a WAF deployment
- Configure detection or prevention mode
- Configure rule sets for WAF on Azure Front Door
- Configure rule sets for WAF on Application Gateway
- Implement a WAF policy
- Associate a WAF policy