Design and Implement Microsoft Azure Networking Solutions (AZ-700)

Duration: 3 Days   Course Code: M-AZ700

Overview:

This course teaches Network Engineers how to design, implement, and maintain Azure networking solutions.
This course covers the process of designing, implementing, and managing core Azure networking infrastructure, Hybrid Networking connections, load balancing traffic, network routing, private access to Azure services, network security and monitoring.
Learn how to design and implement a secure, reliable, network infrastructure in Azure and how to establish hybrid connectivity, routing, private access to Azure services, and monitoring in Azure.

Target Audience:

This course is for Network Engineers looking to specialize in Azure networking solutions.
An Azure Network engineer designs and implements core Azure networking infrastructure, hybrid networking connections, load balance traffic, network routing, private access to Azure services, network security and monitoring. The Azure network engineer will manage networking solutions for optimal performance, resiliency, scale, and security.

Objectives:

- After this course participants should be able to:
- Implement virtual networks
- Configure public IP services
- Design and implement name resolution
- Design and implement cross-VNET connectivity
- Implement virtual network routing
- Design and implement:
- An Azure Virtual Network NAT
- A site-to-site VPN connection
- A point-to-site VPN connection
- Authentication for point-to-site VPN connections
- Azure Virtual WAN
- ExpressRoute
- ExpressRoute Global Reach
- ExpressRoute FastPath
- Troubleshoot ExpressRoute connection issues
- Identify the features and capabilities of Azure Load Balancer
- Design and implement an Azure Load Balancer
- Implement a Traffic Manager profile
- Design and implement Azure Application Gateway
- Implement Azure Front Door
- Get network security recommendations with Microsoft Defender for Cloud
- Deploy Azure DDoS Protection by using the Azure portal
- Design and implement:
- Network security groups (NSGs)
- Azure Firewall
- A web application firewall (WAF) on Azure Front Door
- Explain virtual network service endpoints
- Define Private Link Service and private endpoints
- Integrate private endpoints with DNS
- Design and configure:
- Private endpoints
- Access to service endpoints
- Integrate your App Service with Azure virtual networks
- Configure network health alerts and logging by using Azure Monitor
- Create and configure a Connection Monitor instance
- Configure and use Traffic Analytics
- Configure NSG flow logs
- Enable and configure diagnostic logging

- Configure Azure Network Watcher

Prerequisites:

Successful Azure Network Engineers start this role with experience in enterprise networking, on-premises or cloud infrastructure and network security.

- Understanding of on-premises virtualization technologies, including: VMs, virtual networking, and virtual hard disks.
- Understanding of network configurations, including TCP/IP, Domain Name System (DNS), virtual private networks (VPNs), firewalls, and encryption technologies.
- Understanding of software defined networking.
- Understanding hybrid network connectivity methods, such as VPN.
- Understanding resilience and disaster recovery, including high availability and restore operations.

Testing and Certification

-

Content:

MODULE 1: Introduction to Azure Virtual Networks

- You'll learn how to design and implement core Azure Networking infrastructure such as virtual networks, public and private IPs, DNS, virtual network peering, routing, and Azure Virtual NAT.
- Introduction
- Explore Azure Virtual Networks
- Configure public IP services
- Exercise: Design and implement a virtual network in Azure
- Design name resolution for your virtual network
- Exercise: Configure domain name servers settings in Azure
- Enable cross-virtual network connectivity with peering
- Exercise: Connect two Azure virtual networks using global virtual network peering
- Implement virtual network traffic routing
- Configure internet access with Azure Virtual NAT

MODULE 2: Design and implement hybrid networking

Design and implement hybrid networking solutions such as Site-to-Site VPN connections, Point-to-Site VPN connections, Azure Virtual WAN, and Virtual WAN hubs.

- Introduction
- Design and implement Azure VPN Gateway
- Exercise: Create and configure a virtual network gateway
- Connect networks with Site-to-site VPN connections
- Connect devices to networks with Point-to-site VPN connections
- Connect remote resources by using Azure Virtual WANs
- Exercise: create a Virtual WAN by using the Azure portal
- Create a network virtual appliance (NVA) in a virtual hub

MODULE 3: Design and implement Azure ExpressRoute

- Introduction
- Explore Azure ExpressRoute
- Design an ExpressRoute deployment
- Exercise: configure an ExpressRoute gateway
- Exercise: provision an ExpressRoute circuit
- Configure peering for an ExpressRoute deployment
- Connect an ExpressRoute circuit to a virtual network

You learn the different load balancer options in Azure and how to choose and implement the right Azure solution for non-HTTP(S) traffic.

- Introduction
- Explore load balancing
- Design and implement Azure load balancer using the Azure portal
- Exercise: Create and configure an Azure load balancer
- Explore Azure Traffic Manager
- Exercise: Create a Traffic Manager profile using the Azure portal

MODULE 5: Load balance HTTP(S) traffic in Azure

You learn how to design load balancer solutions for HTTP(S) traffic and how to implement Azure Application Gateway and Azure Front Door.

- Introduction
- Design Azure Application Gateway
- Configure Azure Application Gateway
- Exercise: deploy Azure Application Gateway
- Design and configure Azure Front Door
- Exercise: create a Front Door for a highly available web application

MODULE 6: Design and implement network security

You'll learn to design and implement network security solutions such as Azure DDoS, Network Security Groups, Azure Firewall, and Web Application Firewall.

- Introduction
- Get network security recommendations with Microsoft Defender for Cloud
- Deploy Azure DDoS Protection by using the Azure portal
- Exercise: Configure DDoS Protection on a virtual network using the Azure portal
- Deploy Network Security Groups by using the Azure portal
- Design and implement Azure Firewall
- Exercise: Deploy and configure Azure Firewall using the Azure portal
- Secure your networks with Azure Firewall Manager
- Exercise: secure your virtual hub using Azure Firewall Manager
- Implement a Web Application Firewall on Azure Front Door

MODULE 7: Design and implement private access to Azure Services

You'll learn to design and implement private access to Azure Services with Azure Private Link, and virtual network service endpoints.

- Introduction
- Explain virtual network service endpoints
- Define Private Link Service and private endpoint
- Integrate private endpoint with DNS
- Exercise: Restrict network access to PaaS resources with virtual network service endpoints using the Azure portal
- Exercise: Create an Azure private endpoint using Azure PowerShell

MODULE 8: Design and implement network monitoring

You learn to design and implement network monitoring solutions such as Azure Monitor and Network watcher.

- Introduction
- Monitor your networks using Azure monitor
- Exercise: monitor a load balancer resource using Azure monitor
- Monitor your networks using Azure network watcher
- Summary and resources

- Connect geographically dispersed networks with ExpressRoute global reach
- Improve data path performance between networks with ExpressRoute FastPath
- Troubleshoot ExpressRoute connection issues

MODULE 4: Load balance non-HTTP(S) traffic in Azure

Additional Information:

Official course book provided to participants.

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo