Azure

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

$1,895.00

- 3 Days

Upcoming Dates

Jun 23 - Jun 25
Sep 22 - Sep 24
Dec 01 - Dec 03

Course Description

Learn how to design and implement a secure network infrastructure in Azure and how to establish hybrid connectivity, routing, private access to Azure services, and monitoring in Azure.

Course Outline

Module 1: Introduction to Azure Virtual Networks

In this module you will learn how to design and implement fundamental Azure Networking resources such as virtual networks, public and private IPs, DNS, virtual network peering, routing, and Azure Virtual NAT.

Lessons:

- Explore Azure Virtual Networks
- Configure public IP services
- Design name resolution for your virtual network
- Enable cross-virtual network connectivity with peering
- Implement virtual network traffic routing
- Configure internet access with Azure Virtual NAT

Exercises:

- Design and implement a Virtual Network in Azure
- Configure DNS settings in Azure
- Connect two Azure Virtual Networks using global virtual network peering

After completing this module, students will be able to:

- Implement virtual networks
- Configure public IP services
- Configure private and public DNS zones
- Design and implement cross-VNET connectivity
- Implement virtual network routing
- Design and implement an Azure Virtual Network NAT

Module 2: Design and Implement Hybrid Networking

In this module you will learn how to 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.

Lessons:

- Design and implement Azure VPN 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
- Create a network virtual appliance (NVA) in a virtual hub

Exercises:

- Create a Virtual WAN by using Azure Portal
- Create and configure a virtual network gateway

After completing this module, students will be able to:

- Design and implement a site-to-site VPN connection
- Design and implement a point-to-site VPN connection
- Design and implement Azure Virtual WAN Resources

Module 3: Design and implement Azure ExpressRoute

You learn how to design and implement Azure ExpressRoute, ExpressRoute Global Reach, ExpressRoute FastPath.

Lessons:

- Explore Azure ExpressRoute
- Design an ExpressRoute deployment
- Configure peering for an ExpressRoute deployment
- Connect an ExpressRoute circuit to a virtual network
- Connect geographically dispersed networks with ExpressRoute global reach
- Improve data path performance between networks with ExpressRoute FastPath
- Troubleshoot ExpressRoute connection issues

Exercises:

- Configure an ExpressRoute gateway
- Provision an ExpressRoute circuit

After completing this module, students will be able to:

- Design and implement Expressroute
- Design and implement Expressroute Direct
- Design and implement Expressroute FastPath

Module 4: load balancing non-HTTP(S) traffic in Azure

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

Lessons:

- Explore load balancing

- Design and implement Azure load balancer using the Azure portal
- Explore Azure Traffic Manager

Exercises:

- Create a Traffic Manager profile using the Azure portal
- Create and configure an Azure load balancer

After completing this module, students will be able to:

- Design and implement Azure Load Balancers
- Design and implement Azure Traffic Manager

Module 5: Load balancing 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.

Lessons:

- Design Azure Application Gateway
- Configure Azure Application Gateway
- Configure Azure Application Gateway
- Design and configure Azure Front Door

Exercises:

- Deploy Azure application gateway
- Create a front door for a highly avaiExercisele web application

After completing this module, students will be able to:

- Design and implement Azure Application Gateway
- Implement Azure Front Door

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.

Lessons:

- Get network security recommendations with Microsoft Defender for Cloud
- Deploy Azure DDoS Protection by using the Azure portal
- Deploy Network Security Groups by using the Azure portal
- Design and implement Azure Firewall
- Working with Azure Firewall Manager
- Implement a Web Application Firewall on Azure Front Door

Exercises:

- Deploy and configure Azure Firewall using the Azure portal
- Secure your virtual hub using Azure Firewall Manager
- Configure DDoS Protection on a virtual network using the Azure portal

After completing this module, students will be able to:

- Configure and monitor an Azure DDoS protection plan
- implement and manage Azure Firewall

- Implement network security groups
- Implement a web application firewall (WAF) 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

Lessons:

- Explain virtual network service endpoints
- Define Private Link Service and private endpoint
- Integrate private endpoint with DNS

Exercises:

- Restrict network access to PaaS resources with virtual network service endpoints using the Azure portal
- Create an Azure private endpoint using Azure PowerShell

After completing this module, students will be able to:

- Define the difference between Private Link Service and private endpoints
- Design and configure private endpoints
- Explain virtual network service endpoints
- Design and configure access to service endpoints
- Integrate Private Link with DNS
- Integrate your App Service with Azure virtual networks

Module 8: Design and implement network monitoring

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

Lessons:

- Monitor your networks using Azure monitor
- Monitor your networks using Azure network watcher

Exercise:

- Monitor a load balancer resource by using Azure Monitor

After completing this module, students will be able to:

- 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

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. This role requires communicating and coordinating with vendors. Azure Network Engineers use the Azure Portal and as they become more proficient, they use PowerShell and the Command Line Interface.

Prerequisites

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

- Understanding on-premises virtualization technologies, including virtual networking and VMs
- Understanding network configurations, including TCP/IP, Domain Name System (DNS), 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 regarding networking

What You Will Learn