Microsoft Azure Network Engineer Associate: AZ-700T00

Course Overview

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

Audience Profile

This course is for Network Engineers looking to specialize in Azure networking solutions. intermediate administrator, network engineer, application gateway, DNS, express route, firewall, firewall manager, front door, load balancer, network watcher, private link, traffic manager, virtual network, virtual WAN and VPN Gateway

Skills Gained

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

Prerequisites

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

- You should have experience with networking concepts, such as IP addressing, Domain Name System (DNS), and routing
- You should have experience with network connectivity methods, such as VPN or WAN
- You should have experience with the Azure portal and Azure PowerShell

Duration: 18hrs (6 x 3hrs)

Course Outline

Module 1: Explore Azure Virtual Networks

In this module you will learn about Azure Virtual Networks (VNets) are the fundamental building block of your private network in Azure. VNets enable you to build complex virtual networks that are similar to an on-premises network, with additional benefits of Azure infrastructure such as scale, availability, and isolation.

A VNet is a representation of your own network in the cloud. It is a logical isolation of the Azure cloud dedicated to your subscription.

Lessons

- Capabilities of Azure Virtual Network
- Design considerations for Azure Virtual Network
- Determine a naming convention
- Understand regions and subscriptions
- Azure Availability Zones
- Create a virtual network in Azure

Lab: Exercise: Create the Contoso resource group

Lab: Exercise: Create the CoreServicesVnet virtual network and subnets

Lab: Exercise: Create the ManufacturingVnet virtual network and subnets

Lab: Exercise: Create the ResearchVnet virtual network and subnets

Lab: Exercise: Verify the creation of VNets and Subnets

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

Lab: Exercise: create a Virtual WAN by using Azure Portal

Lab: Exercise: 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

In this module you will learn how to design and implement Azure ExpressRoute, ExpressRoute Global Reach, ExpressRoute FastPath and ExpressRoute Peering options.

Lessons

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

Lab: Exercise: configure an ExpressRoute gateway

Lab: Exercise: 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

In this module you will learn how to design and implement load balancing solutions for non-HTTP(S) traffic in Azure with Azure Load balancer and Traffic Manager.

Lessons

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

Lab: Exercise: create a Traffic Manager profile using the Azure portal

Lab: Exercise: 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

In this module you will learn how to design and implement load balancing solutions for HTTP(S) traffic in Azure with Azure Application gateway and Azure Front Door.

Lessons

- Design Azure application gateway
- Configure Azure application gateway
- Design and configure Azure front door

Lab: Exercise: deploy Azure application gateway

Lab: Exercise: create a front door for a highly available 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

In this module you will learn to design and imponent network security solutions such as Azure DDoS, Azure Firewalls, Network Security Groups, and Web Application Firewall.

Lessons

- Secure your virtual networks in the Azure portal
- 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

Lab: Exercise: deploy and configure Azure Firewall using the Azure portal

Lab: Exercise: secure your virtual hub using Azure Firewall Manager

Lab: Exercise: 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

In this module you will 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 Link with DNS
- Integrate your App Service with Azure virtual networks

Lab: Exercise: restrict network access to PaaS resources with virtual network service endpoints

Lab: Exercise: create an Azure private endpoint using Azure PowerShell

After completing this module, students will be able to:

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

Module 8: Design and implement network monitoring

In this module you will learn to design and implement network monitoring solutions such as Azure Monitor and Network watcher.

Lessons

- Monitor your networks with Azure Monitor
- Monitor your networks with Azure Network Watcher

Lab: 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