

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

Module 1: 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

- Azure Virtual Networks
- Public IP services
- public and private DNS
- cross-VNet connectivity
- Virtual Network Routing
- Azure virtual Network NAT

Lab : Design and implement a Virtual Network in Azure

Lab : Configure DNS settings in Azure

Lab : Connect Virtual Networks with 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

- Site-to-site VPN connection
- Point-to-Site VP connections
- Azure Virtual WAN

Lab : Create and configure a local gateway

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

Design and implement a site-to-site VPN connection

- Design and implement a point-to-site VPN connection
- Design and implement authentication
- 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

- ExpressRoute
- ExpressRoute Direct
- ExpressRoute FastPath
- ExpressRoute Peering

Lab : Create and configure ExpressRoute

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

- Content Delivery and Load Blancing
- Azure Load balancer
- Azure Traffic Manager
- Azure Monitor
- Network Watcher

Lab : Create and configure a public load balancer to load balance VMs using the Azure portal

Lab : Create a Traffic Manager Profile using the Azure portal

Lab : Create, view, and manage metric alerts in Azure Monitor

Design and implement Azure Laod Balancers

- Design and implement Azure Traffic Manager
- Monitor Networks with Azure Monitor
- Use Network Watcher

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

- Azure Application Gateway

- Azure Front Door

Lab : Create a Front Door for a highly available web application using the Azure portal

Lab : Create and Configure an Application Gateway

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 implement network security solutions such as Azure DDoS, Azure Firewalls, Network Security Groups, and Web Application Firewall.

Lessons

- Azure DDoS Protection
- Azure Firewall
- Network Security Groups
- Web Application Firewall on Azure Front Door

Lab : Create a Virtual Network with DDoS protection plan

Lab : Deploy and Configure Azure Firewall

Lab : Create a Web Application Firewall policy on Azure Front Door

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

- Define Azure Private Link and private endpoints
- Design and Configure Private Endpoints
- Integrate a Private Link with DNS and on-premises clients
- Create, configure, and provide access to Service Endpoints
- Configure VNET integration for App Service

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

Lab : create an Azure private endpoint

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

Azure Sentinel course outline

Day 1:

Introduction to Azure Analytics
Introduction to Azure Sentinel
Traditional SIEM vs Cloud native SIEM
Phases of Azure Sentinel
Introduction to Workbook
Phase 1 : Collect
Data Collection
Visualization
Querying the logs
Introduction to Kusto Query Language (KQL)
useful Queries in KQL
Advanced Queries in KQL
Lab

Day 2:

Phase 2: Detect
Detecting Threats using correlation Rules.
Out of the box Detection
Custom threat detection rules
Advanced multistage attack detection
Intro to Use cases
Real time use cases for Cloud
User Behavior related use cases
Introduction to Threat hunting
Life cycle of Threat hunting
Use Note books to hunt
Lab

Day 3:

Phase 3: Investigate
Introduction to Threat investigation
Investigating Incidents
Use the investigation graph to deep dive
Phase 4: Respond
Introduction to SOAR
Introduction to Play Books
Creating Security Play Books
Creating Logic through Logic App Designer
Threat Response Automation
Lab