

Azure

Networking

Master Azure networking by learning to design, secure, and manage scalable cloud network solutions aligned with **AZ-700 certification**.

Who It's For

- This course is designed for IT professionals, cloud engineers, network administrators, and students who want to build strong expertise in **Azure networking**.
- It is also ideal for **beginners** aiming to start a career in cloud networking as well as **professionals** preparing for the AZ-700 certification.

What You'll Learn

- You will learn how to **design, implement, and manage** Azure networking solutions including virtual networks, secure connectivity, load balancing, traffic routing, and advanced security services.
- The course also covers **real-world architectures**, high availability, and **scalable networking solutions** in Azure.

Benefits You'll Gain

- By completing this course, you will gain hands-on Azure networking skills, improve your job readiness for cloud roles, and confidently prepare for the AZ-700 certification exam.
- You will also be able to design secure, scalable, and highly available cloud network architectures used in real-world environments.

Course Details

- **Duration:** 25 days (1 hour per day)
- **Mode:** Fully online – attend live
- **Start Date:** Flexible enrollment – begin anytime!

Topics that will be covered

Explore Azure Virtual Networks

- ◆ Understanding Infrastructure as Code
- ◆ Why we need Infrastructure as Code
- ◆ What is Terraform and its benefits
- ◆ Challenges with the traditional approach
- ◆ Terraform workflow
- ◆ Installing Terraform

Internet Protocol Configuration

- ◆ Configure private Internet Protocol addresses (static and dynamic)
- ◆ Configure public Internet Protocol addresses
- ◆ Associate Internet Protocol configurations with network interface cards

Domain Name System Configuration

- ◆ Configure Azure-provided Domain Name System name resolution
- ◆ Configure custom Domain Name System servers
- ◆ Configure name resolution between on-premises networks and Azure virtual networks

Network Security Group Configuration

- ◆ Create and manage Network Security Groups
- ◆ Configure inbound security rules
- ◆ Configure outbound security rules
- ◆ Associate Network Security Groups with subnets and network interface cards
- ◆ Configure service tags and rule priorities

Cross V-Net Connectivity Using Virtual Network Peering

- ◆ Configure virtual network peering within the same region
- ◆ Configure global virtual network peering between regions
- ◆ Configure gateway transit and use of remote gateways
- ◆ Understand traffic flow over Microsoft backbone network

Secure Access to Virtual Machines Using Azure Bastion

- ◆ Deploy Azure Bastion
- ◆ Configure secure Remote Desktop Protocol access
- ◆ Configure secure Secure Shell access
- ◆ Remove public Internet Protocol addresses from virtual machines

Implement Network Security Using Azure Firewall

- ◆ Deploy Azure Bastion
- ◆ Configure secure Remote Desktop Protocol access
- ◆ Configure secure Secure Shell access
- ◆ Remove public Internet Protocol addresses from virtual machines

Implement Virtual Private Network Gateway Connectivity

- ◆ Deploy VPN Gateway
- ◆ Configure Site-to-Site Virtual Private Network connections
- ◆ Configure Point-to-Site Virtual Private Network connections
- ◆ Configure Virtual Network to Virtual Network connectivity
- ◆ Configure Internet Protocol Security and Internet Key Exchange policies

Virtual Machine Service Level Agreement and Availability

- ◆ Understand Service Level Agreement for virtual machines
- ◆ Design for high availability
- ◆ Compare single virtual machine, availability set, and availability zone Service Level Agreements

Availability Set and Availability Zone Design

- ◆ Design fault domains and update domains
- ◆ Deploy virtual machines in availability sets
- ◆ Deploy virtual machines across availability zones
- ◆ Understand regional availability zone support

Load Balancer Configuration

- ◆ Deploy Azure Load Balancer
- ◆ Configure public load balancer
- ◆ Configure internal load balancer
- ◆ Configure health probes
- ◆ Configure inbound Network Address Translation rules

Traffic Manager Configuration

- ◆ Deploy Azure Traffic Manager
- ◆ Configure performance routing method
- ◆ Configure priority routing method
- ◆ Configure geographic routing method
- ◆ Configure endpoint monitoring

Application Gateway Configuration

- ◆ Deploy Azure Application Gateway
- ◆ Configure Hypertext Transfer Protocol and Hypertext Transfer Protocol Secure listeners
- ◆ Configure path-based routing rules
- ◆ Configure Secure Sockets Layer termination
- ◆ Integrate Web Application Firewall with Application Gateway

Automatic Scaling Configuration

- ◆ Deploy Azure Application Gateway
- ◆ Configure Hypertext Transfer Protocol and Hypertext Transfer Protocol Secure listeners
- ◆ Configure path-based routing rules
- ◆ Configure Secure Sockets Layer termination
- ◆ Integrate Web Application Firewall with Application Gateway

Virtual Machine Scale Set Configuration

- ◆ Deploy Azure Application Gateway
- ◆ Configure Hypertext Transfer Protocol and Hypertext Transfer Protocol Secure listeners
- ◆ Configure path-based routing rules
- ◆ Configure Secure Sockets Layer termination
- ◆ Integrate Web Application Firewall with Application Gateway

Front Door Configuration

- ◆ Deploy Azure Front Door
- ◆ Configure global Hypertext Transfer Protocol and Hypertext Transfer Protocol Secure routing
- ◆ Configure Secure Sockets Layer offloading
- ◆ Configure Web Application Firewall policies
- ◆ Configure endpoint health probes

Distributed Denial of Service Protection

- ◆ Configure Distributed Denial of Service Protection Standard
- ◆ Protect virtual networks

- ◆ Monitor Distributed Denial of Service attack metrics
- ◆ Review attack analytics and reports

Virtual Network Traffic Routing

- ◆ Understand system routes
- ◆ Configure user-defined routes
- ◆ Configure forced tunnelling through firewall or network virtual appliance
- ◆ Configure next hop routing

Network Address Translation Gateway Configuration Azure

- ◆ Deploy NAT Gateway
- ◆ Configure outbound Internet connectivity
- ◆ Configure static public Internet Protocol addresses
- ◆ Understand Network Address Translation Gateway limitations

Virtual Wide Area Network Configuration

- ◆ Deploy NAT Gateway
- ◆ Configure outbound Internet connectivity
- ◆ Configure static public Internet Protocol addresses
- ◆ Understand Network Address Translation Gateway limitations

Microsoft Defender for Cloud Configuration

- ◆ Deploy NAT Gateway
- ◆ Configure outbound Internet connectivity
- ◆ Configure static public Internet Protocol addresses

- ◆ Understand Network Address Translation Gateway limitations

Azure Private Endpoint Configuration

- ◆ Deploy Azure Private Endpoint
- ◆ Configure private access to Platform as a Service resources
- ◆ Configure private Domain Name System zones
- ◆ Disable public network access for services

Service Endpoints Configuration

- ◆ Configure virtual network service endpoints
- ◆ Restrict service access to selected virtual networks
- ◆ Compare service endpoints with private endpoints
- ◆ Implement service endpoint policies

Web Application Firewall Configuration

- ◆ Deploy Web Application Firewall with Application Gateway
- ◆ Deploy Web Application Firewall with Front Door
- ◆ Configure detection mode and prevention mode
- ◆ Protect against Open Web Application Security Project Top Ten vulnerabilities

To Join this Course Contact or Ping on Whatsapp : [93427 37660](https://www.whatsapp.com/channel/002919342737660)