Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow Enterprise Computing Solutions Ltd, Part 1st Floor, Suite 1D/1, Central House, Otley Road, Harrogate, HG3 1UG

Email: educationteam.ecs.uk@arrow.com
Phone: 0870 251 1000

Designing and Implementing Microsoft Azure Networking Solutions

CODE: MCS_AZ-700T00

LENGTH: 24 Hours (3 days)

Description

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.

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.

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.

Prerequisite courses (or equivalent knowledge and hands-on experience):
This free online training will give you the experience you need to be successful in this course.

- Azure Fundamentals part 1: Describe core Azure concepts - Learn | Microsoft Docs

- Azure Fundamentals part 2: Describe core Azure services - Learn | Microsoft Docs
- Azure Fundamentals part 3: Describe core solutions and management tools on Azure - Learn | Microsoft Docs
- Azure Fundamentals part 4: Describe general security and network security features - Learn | Microsoft Docs
- AZ-104: Configure and manage virtual networks for Azure administrators - Learn | Microsoft Docs

Programme

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 imponent 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

Additional Information

This training is also available as onsite training. Please contact us to find out more.