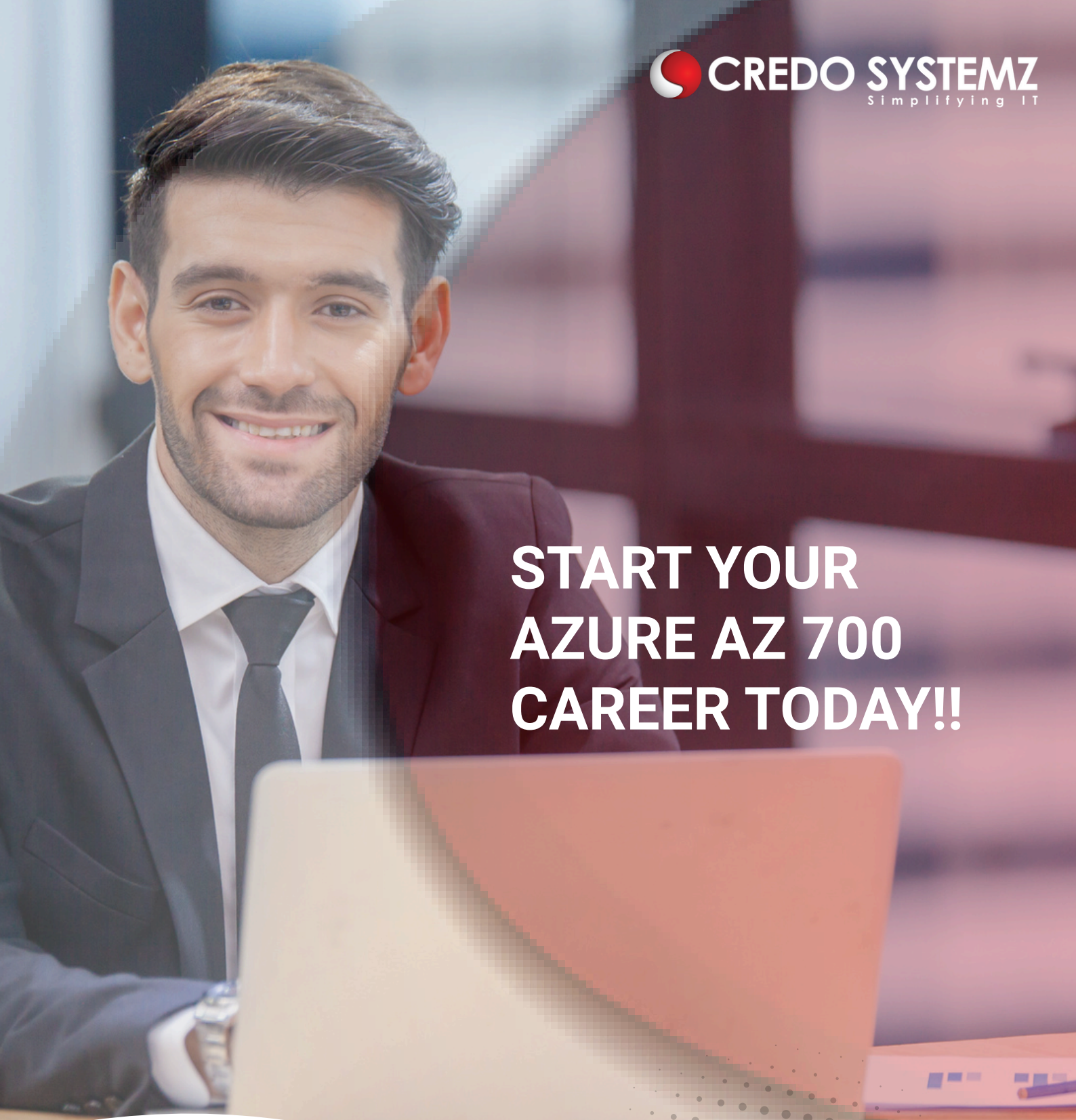


CREDO SYSTEMZ

Azure Network Solutions Program

Capstone Projects :

Real Time Business Scenario using
Azure Network Solutions

Design a Hub-and-Spoke Network Topology

Set up a hub VNet with shared services (e.g., firewalls, DNS), and connect multiple spoke VNets using peering. Implement custom routing and security rules.

Configure Azure VPN Gateway for Site-to-Site VPN

Simulate an on-premises environment and establish a secure site-to-site VPN tunnel to Azure. Validate the connection and troubleshoot common issues.

Implement Azure Application Gateway with WAF

Deploy a web app behind an Azure Application Gateway with WAF enabled. Configure routing rules, SSL termination, and test security policies.

Deploy Azure Front Door for Global Web Traffic

Use Azure Front Door to distribute traffic across multiple app instances in different regions. Configure URL-based routing and enable HTTPS.

Set Up Private Link and Service Endpoints

Connect Azure services like Storage or SQL to a VNet privately. Compare Private Link vs Service Endpoints and test access from the VNet.

Design and Implement Azure ExpressRoute

Plan and simulate ExpressRoute configuration for enterprise-grade private connectivity. Understand ExpressRoute circuits, routing, and redundancy.

AZURE NETWORK SOLTIONS
COURSE SYLLABUS

Duration : 40 hrs

Section 1 : Design and implement private IP addressing for Azure resources

- IPlan and implement network segmentation and address spaces
- Create a virtual network (VNet)
- Plan and configure subnetting for services, including VNet gateways, private endpoints, firewalls, application gateways, VNet-integrated platform services, and Azure Bastion
- Plan and configure subnet delegation
- Create a prefix for public IP addresses
- Choose when to use a public IP address prefix
- Plan and implement a custom public IP address prefix (bring your own IP)
- Create a new public IP address
- Associate public IP addresses to resources

Section 2 : Design and implement name resolution

- Design name resolution inside a VNet
- Configuration of DNS settings for a VNet
- Design public DNS zones
- Design private DNS zones
- Configuration of a public or private DNS zone
- Link a private DNS zone to a VNet

Section 3 : Design and implement VNet connectivity and routing

- Design service chaining, including gateway transit
- Design virtual private network (VPN) connectivity between VNets
- Implement VNet peering
- Design and implement user-defined routes (UDRs)

- Associate a route table with a subnet
- Configuration of forced tunneling
- Diagnose and resolve routing issues
- Design and implementation of Azure Route Server
- Identify appropriate use cases for a Virtual Network NAT gateway
- Implement a NAT gateway

Section 4 : Monitor networks

- Develop batch processing solutions by using
- Configuration of monitoring, network diagnostics, and logs in Azure Network Watcher
- Monitor and repair network health by using Azure Network Watcher
- Activate and monitor distributed denial-of-service (DDoS) protection
- Activate and monitor Microsoft Defender for DNS

Section 5 : Design, implement, and manage a site-to-site VPN connection

- Design a site-to-site VPN connection, including for high availability
- Select an appropriate VNet gateway SKU for site-to-site VPN requirements
- Implementation of a site-to-site VPN connection
- Identify when to use a policy-based VPN versus a route-based VPN connection
- Create and configure an IPsec/IKE policy
- Diagnose and resolve virtual network gateway connectivity issues
- Implement Azure Extended Network

Section 6 : Design, implement, and manage a point-to-site VPN connection

- Select an appropriate virtual network gateway SKU for point-to-site VPN requirements
- Select and configure a tunnel type
- Select an appropriate authentication method
- Configure RADIUS authentication

- Configuration of certificate-based authentication
- Configuration of an authentication by using Azure Active Directory (Azure AD), part of Microsoft Entra
- Implementation of a VPN client configuration file
- Diagnose and resolve client-side and authentication issues
- Specify Azure requirements for Always On authentication
- Specify Azure requirements for Azure Network Adapter

Section 7 : Design, implement, and manage Azure ExpressRoute

- Select an ExpressRoute connectivity model
- Select an appropriate ExpressRoute SKU and tier
- Design and implement ExpressRoute to meet requirements, including cross-region connectivity, redundancy, and disaster recovery
- Design and implement ExpressRoute options, including Global Reach, FastPath, and ExpressRoute Direct
- Choose between private peering only, Microsoft peering only, or both
- Configuration of private peering
- Configuration of Microsoft peering
- Create and configure an ExpressRoute gateway
- Connect a virtual network to an ExpressRoute circuit
- Recommend a route advertisement configuration
- Configuration of encryption over ExpressRoute
- Implementation of Bidirectional Forwarding Detection
- Diagnose and resolve ExpressRoute connection issues

Section 8 : Design and implement an Azure Virtual WAN architecture

- Select a Virtual WAN SKU
- Design a Virtual WAN architecture, including selecting types and services
- Create a hub in Virtual WAN
- Choose an appropriate scale unit for each gateway type
- Deploy a gateway into a Virtual WAN hub

- Choose an appropriate scale unit for each gateway type
- Deploy a gateway into a Virtual WAN hub
- Configuration of virtual hub routing
- Create a network virtual appliance (NVA) in a virtual hub
- Integrate a Virtual WAN hub with a third-party NVA

Section 9 : Design and implement an Azure Load Balancer

- Map requirements to features and capabilities of Azure Load Balancer
- Identify appropriate use cases for Azure Load Balancer
- Choose an Azure Load Balancer SKU and tier
- Choose between public and internal
- Create and configure an Azure Load Balancer
- Implementation of a load balancing rule
- Create and configure inbound NAT rules
- Create and configure explicit outbound rules, including SNAT

Section 10 : Design and implement Azure Application Gateway

- Map requirements to features and capabilities of Azure Application Gateway
- Identify appropriate use cases for Azure Application Gateway
- Create a back-end pool
- Configure health probes
- Configure listeners
- Configure routing rules
- Configuration of HTTP settings
- Configure Transport Layer Security (TLS)
- Configure rewrite sets

Section 11 : Design and implement Azure Front Door

- Map requirements to features and capabilities of Azure Front Door
- Identify appropriate use cases for Azure Front Door
- Choose an appropriate tier

- Configure an Azure Front Door, including routing, origins, and endpoints
- Configure SSL termination and end-to-end SSL encryption
- Configure caching
- Implement rules, URL rewrite, and URL redirect

Section 12 : Design and implement Azure Traffic Manager

- Identify appropriate use cases for Azure Traffic Manager
- Configure a routing method
- Configure endpoints

Section 13 : Design and implement Azure Private Link service and Azure private endpoints

- Create a Private Link service
- Integrate a Private Link service with DNS
- Plan private endpoints
- Create private endpoints
- Configure access to Azure resources by using private endpoints
- Connect on-premises clients to a private endpoint

Section 14 : Design and implement service endpoints

- Choose when to use a service endpoint
- Create service endpoints

Section 15 : Implement and manage network security groups

- Create a network security group (NSG)
- Associate an NSG to a resource
- Create an application security group (ASG)
- Associate an ASG to a network interface card (NIC)
- Create and configure NSG rules
- Interpret NSG flow logs
- Validate NSG flow rules
- Verify IP flow

Section 16 : Design and implement Azure Firewall and Azure Firewall Manager

- Map requirements to features and capabilities of Azure Firewall
- Select an appropriate Azure Firewall SKU
- Design an Azure Firewall deployment
- Create and implement an Azure Firewall deployment
- Configure Azure Firewall rules
- Create and implement Azure Firewall Manager policies

Section 17 : Design and implement a Web Application Firewall (WAF) deployment

- Map requirements to features and capabilities of WAF
- Design a WAF deployment
- Configure detection or prevention mode
- Configure rule sets for WAF on Azure Front Door
- Configure rule sets for WAF on Application Gateway
- Implement a WAF policy

SKILLS AND TOOLS

Tools Covered

Azure Portal

Azure Monitor

Network Watcher

Azure Firewall

Web Application Firewall

DDoS Protection

Virtual WAN

Skills Covered

Networking Infrastructure

Connectivity Services

Hybrid Connectivity

Application Delivery Services

Private Access

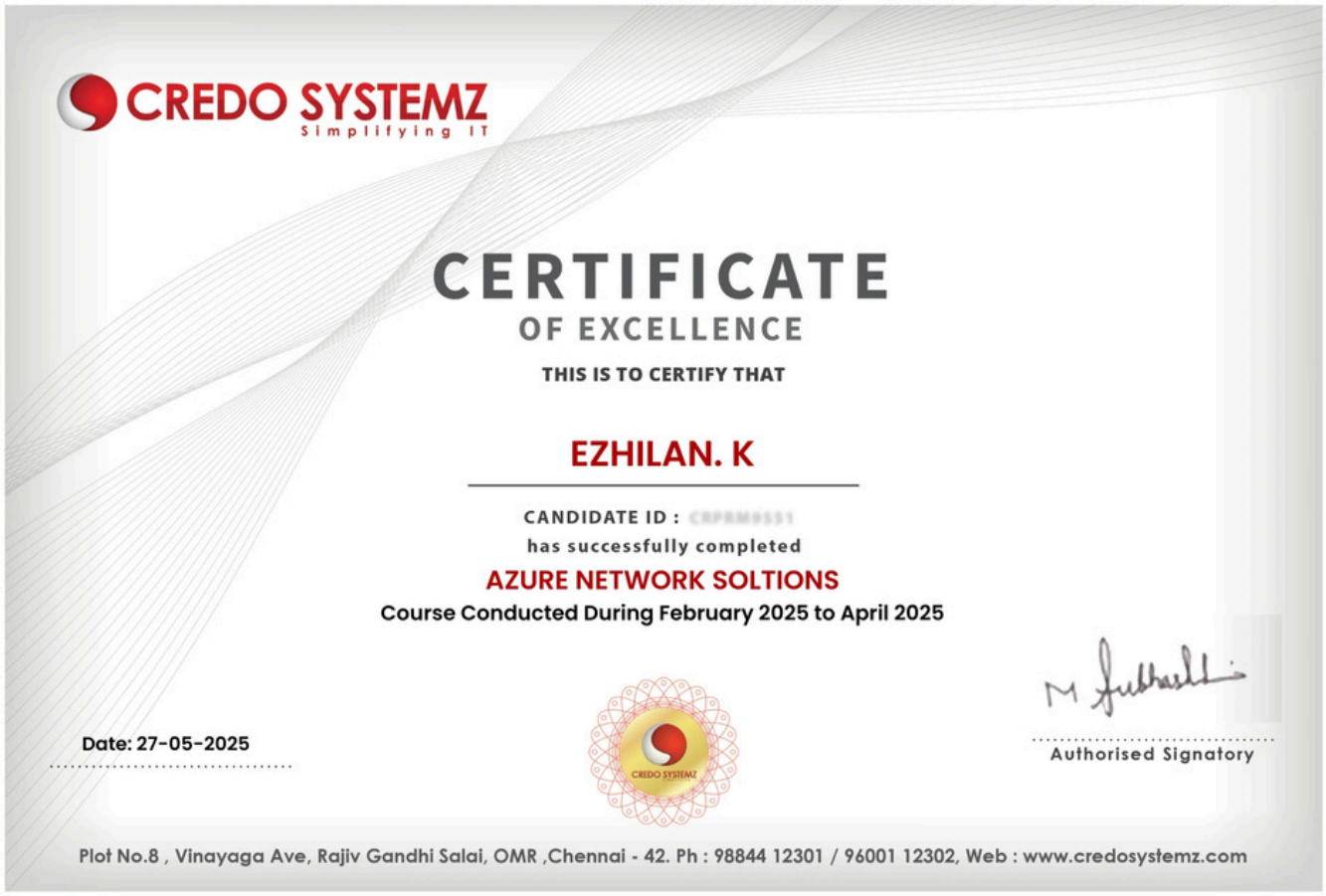
Network Security

Monitoring

Troubleshooting

Earn your AZ 700 Course Completion Certificate

Credo Systemz's certificate is highly recognized by 30K Global companies around the world.


CREDO SYSTEMZ
Simplifying IT

CERTIFICATE
OF EXCELLENCE

THIS IS TO CERTIFY THAT

EZHILAN. K

CANDIDATE ID : [redacted]
has successfully completed
AZURE NETWORK SOLTIONS
Course Conducted During February 2025 to April 2025

Date: 27-05-2025

Authorised Signatory

Plot No.8 , Vinayaga Ave, Rajiv Gandhi Salai, OMR ,Chennai - 42. Ph : 98844 12301 / 96001 12302, Web : www.credosystemz.com

WHAT OUR TRAINEE SAYS?

Jhanvi

4.7 ★★★★½

The trainer explained cloud concepts clearly with real-life examples, making it easy to understand for beginners. Practice sessions and doubt clearing were really helpful for building a strong foundation.

Nirosha

4.2 ★★★★½

The course was well-structured with hands-on labs for each topic, which improved my practical skills. The trainer's guidance on managing Azure resources and services was excellent.

Karthik M

5.0 ★★★★★

The sessions focused on design patterns, architecture scenarios, and case studies that matched the exam syllabus. The instructor made complex concepts simple with diagrams and live use cases.

Srinivasan

4.9 ★★★★½

The training covered pipelines, CI/CD, and DevOps practices in a very practical way. Tools like Azure DevOps and GitHub Actions were taught with real-time project examples.

Priya

4.0 ★★★★

Security topics like IAM, Defender for Cloud, and Key Vault were explained with clarity. Lab exercises boosted my confidence to handle security tasks in a real environment.

Renuka Devi

4.5 ★★★★½

Networking concepts like VNets, VPNs, and routing were made easy with step-by-step labs. The trainer's deep knowledge and support throughout the course were very helpful.

CHENNAI

VELACHERY

New # 30, Old # 16A, Third Main Road, Rajalakshmi Nagar, Velachery, (Opp. to Murugan Kalyana Mandapam), Chennai – 600 042.

+91 98844 12301

OMR

Plot No.8, Vinayaga Avenue, Rajiv Gandhi Salai, (OMR), Okkiampettai, (Behind Okkiyampet Bus Stop) Chennai – 600 097.

+91 96001 12302

OVERSEAS

USA

Houchin Drive, Franklin, TN -37064. Tennessee

UAE

Sima Electronic Building, LLH Opposite, Electra Street – Abu Dhabi