Azure Networking Workshop Training

Duration: **1 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Azure Networking Workshop is a **one-day, instructor-led and hands-on programme** designed for IT professionals who want to develop practical skills in implementing, securing and managing networking solutions within Microsoft Azure.

The course begins with the core components of Azure networking and progresses through virtual network design, IP addressing, subnet management, network segmentation, hybrid connectivity and network security. Participants combine conceptual learning with practical configuration activities to understand how these services operate within a modern Azure environment.

Throughout the workshop, learners gain experience with technologies including**Azure Virtual Networks, Network Security Groups, Azure Firewall, NAT Gateway, Azure Bastion and Just-in-Time access**. The programme also introduces network monitoring and troubleshooting using Azure Monitor and Network Watcher.

By the end of the workshop, participants will have developed practical skills for deploying and managing Azure networking solutions that can support secure and manageable cloud infrastructure.

Prerequisites

Participants should have:

- A working understanding of Microsoft Azure fundamentals
- Knowledge of TCP/IP networking concepts
- Familiarity with Windows Server administration and networking
- An understanding of fundamental cloud computing concepts
- Basic familiarity with the Azure Portal

Previous basic experience with the Azure Portal is recommended to gain the most from the hands-on activities.

Who Should Attend

This course is particularly suitable for:

- Azure Administrators
- Network Engineers transitioning to Microsoft Azure
- Cloud Infrastructure Engineers
- Systems Administrators responsible for Azure environments
- IT professionals who design, implement or support Azure networking solutions

Azure Networking Workshop Training

Duration: **1 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of the workshop, participants will be able to:

- Design and configure Azure Virtual Networks
- Manage subnet structures and IP addressing
- Connect Azure networks using Virtual Network Peering
- Implement network segmentation
- Understand hybrid connectivity between Azure and on-premises environments
- Deploy and configure NAT Gateway
- Apply network security controls using Network Security Groups and Azure Firewall
- Incorporate Zero Trust principles into Azure network security
- Monitor network performance using Azure Monitor and Network Watcher
- Apply Microsoft-recommended practices when designing and managing Azure network infrastructure

Outline

1. Introduction to Azure Networking

Begin by exploring the overall structure of networking within Microsoft Azure.

- Azure networking architecture
- Core Azure networking services
- Virtual Network design principles
- Preparing an Azure networking environment
- Understanding relationships between network resources

2. Azure Virtual Networks

Explore the Virtual Network services that form the foundation of networking within Azure.

- Creating Azure Virtual Networks
- Configuring VNets
- Creating and managing subnets
- IP addressing
- Virtual Network Peering
- Network segmentation
- Controlling communication between network segments

This section focuses on building network structures that logically separate Azure resources while supporting the required communication paths.

3. Hybrid Connectivity

Examine how Azure environments can communicate with existing on-premises infrastructure.

- Azure-to-on-premises connectivity
- Hybrid networking concepts
- Connecting cloud and existing infrastructure

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- Evaluating hybrid connectivity requirements

4. Network Security

Explore the security technologies and controls used to protect Azure network resources and regulate traffic.

Network Security Groups

- Configuring NSGs
- Controlling network traffic
- Applying network access rules

Azure NAT Gateway

- Understanding the purpose of NAT Gateway
- Deploying NAT Gateway
- Integrating NAT Gateway into Azure network designs

Azure Firewall

- Using Azure Firewall
- Protecting Azure network resources
- Applying centralised traffic controls

Zero Trust Networking

- Understanding Zero Trust in a networking context
- Restricting access appropriately
- Applying Zero Trust principles to Azure networking

The practical workshop also provides exposure to **Azure Bastion** and **Just-in-Time access** as part of securing administrative and network access.

5. Monitoring and Troubleshooting

Learn how to monitor Azure networking infrastructure and investigate operational problems.

- Monitoring network performance with Azure Monitor
- Using Network Watcher
- Assessing network health
- Investigating connectivity and network issues
- Using monitoring information during troubleshooting

Hands-On Workshop

The programme is designed around practical learning. Participants configure and explore Azure networking technologies throughout the session.

Hands-on activities focus on technologies including:

Azure Networking Workshop Training

Duration: **1 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- Azure Virtual Networks
- Network Security Groups
- Azure Firewall
- NAT Gateway
- Azure Bastion
- Just-in-Time access

This practical approach helps participants finish the workshop with both an understanding of Azure networking concepts and direct experience of how key network components can work together within a cloud environment.