

MS-AZ1002: CONFIGURE SECURE ACCESS TO YOUR WORKLOADS USING NETWORKING WITH AZURE VIRTUAL NETWORK



DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
1 Day	Intermediate	Azure	Instructor-led	NA

INTRODUCTION

In this learning path, you practice deploying containers, container orchestration, and managing clusters on Azure Kubernetes Service. The skills validated include deploying, configuring, and scaling an Azure Kubernetes Service cluster. Also, deploying an Azure Container Registry instance and deploying an application into an Azure Kubernetes Service cluster.

AUDIENCE PROFILE

This course is designed for IT professionals who are responsible for managing and securing network connectivity in Azure environments. The primary audience includes:

- Azure Administrators: Those who manage cloud services that span storage, networking, and compute cloud capabilities.
- Virtual Desktop Administrators: Professionals who manage virtual desktop environments and need to ensure secure access and connectivity.
- Network Engineers: Individuals who design and implement network solutions, focusing on secure access and communications within Azure.

PREREQUISITES

Before attending this course, delegates must have:

- Experience using the Azure portal to create resources.
- Basic knowledge of security concepts like identities, permissions, and encryption.
- Basic knowledge of networking concepts like virtual networks and subnetting.
- Basic knowledge of Azure Policy and Azure Kubernetes Service concepts.

COURSE OBJECTIVES

After completing this course, delegates will be able to:

- Configure Virtual Networks: Learn to create and configure virtual networks and subnets, including IP addressing.
- Azure Virtual Network Peering: Understand how to configure Azure Virtual Network peering connections and address transit and connectivity concerns.
- Traffic Management: Control Azure virtual network traffic by implementing custom routes and deploying network virtual appliances.
- DNS Configuration: Host your domain on Azure DNS and configure DNS settings.
- Network Security Groups: Implement and manage network security groups (NSGs) and application security groups.
- Azure Firewall: Learn to deploy and manage Azure Firewall to protect Azure Virtual Network resources.

COURSE CONTENT

Module 1: Configure virtual networks

Learn to configure virtual networks and subnets, including IP addressing.

Lessons

- Introduction.
- Azure Kubernetes Service.

- Azure Kubernetes cluster architecture.
- Azure Kubernetes Service pods.
- Nodes and node pools for Azure Kubernetes Service.
- Namespaces for Azure Kubernetes Service.
- Access to Azure Kubernetes Service.

- Monitoring and logging for Azure Kubernetes Service.
- Knowledge check.
- Summary.

By the end of this module, you'll be able to:

- Describe control plane nodes, node pools, and workload

- resources like pods, deployments, and sets.
- Scheduling of fault-tolerant application workloads using Azure Kubernetes Service.
- Managing deployment and core management tasks, like upgrade coordination using Azure Kubernetes Service.
- Clustering of virtual or on-premises machines called nodes that share compute, network, and storage resources.

Module 2: Configure Azure Virtual Network Peering

Learn to configure an Azure Virtual Network peering connection and address transit and connectivity concerns.

Lessons

- Introduction.
- Determine Azure Virtual Network peering uses.
- Determine gateway transit and connectivity.
- Create virtual network peering.
- Extend peering with user-defined routes and service chaining.
- Interactive lab simulation.
- Knowledge check.
- Summary and resources.

By the end of this module, you'll be able to:

- Identify usage cases and product features of Azure Virtual Network peering.
- Configure your network to implement Azure VPN Gateway for transit connectivity.
- Extend peering by using a hub and spoke network with user-defined routes and service chaining.

Module 3: Manage and control traffic flow in your Azure deployment with routes

Learn how to control Azure virtual network traffic by implementing custom routes.

Lessons

- Introduction.
- Identify routing capabilities of an Azure virtual network.
- Exercise - Create custom routes.
- What is an NVA?
- Exercise - Create an NVA and virtual machines.
- Exercise - Route traffic through the NVA.
- Summary.

By the end of this module, you'll be able to:

- Identify the routing capabilities of an Azure virtual network.

- Configure routing within a virtual network.
- Deploy a basic network virtual appliance.
- Configure routing to send traffic through a network virtual appliance.

Module 4: Host your domain on Azure DNS

Create a DNS zone for your domain name. Create DNS records to map the domain to an IP address. Test that the domain name resolves to your web server.

Lessons

- Introduction.
- What is Azure DNS?
- Configure Azure DNS to host your domain.
- Exercise - Create a DNS zone and an A record by using Azure DNS.
- Dynamically resolve resource name by using alias record.
- Exercise - Create alias records for Azure DNS.
- Summary.

By the end of this module, you'll be able to:

- Configure Azure DNS to host your domain.

Module 5: Configure network security groups

Learn how to implement network security groups and ensure network security group rules are correctly applied.

Lessons

- Introduction.
- Implement network security groups.
- Determine network security group rules.
- Determine network security group effective rules.
- Create network security group rules.
- Implement application security groups.
- Interactive lab simulation.
- Knowledge check.
- Summary and resources.

By the end of this module, you'll be able to:

- Determine when to use network security groups.
- Create network security groups.
- Implement and evaluate network security group rules.
- Describe the function of application security groups.

Module 6: Introduction to Azure Firewall

Describe how Azure Firewall protects Azure Virtual Network resources, including the Azure Firewall features, rules, deployment options, and administration with Azure Firewall Manager.

Lessons

- Introduction.
- What is Azure Firewall?
- How Azure Firewall works.
- When to use Azure Firewall.
- When to use Azure Firewall Premium.
- Knowledge check.
- Summary.

By the end of this module, you'll be able

- Explain how Azure Firewall and Azure Firewall Manager work together to protect Azure virtual networks.
- Evaluate whether Azure Firewall is the right solution to protect your Azure virtual networks from malicious incoming and outgoing traffic.
- Evaluate whether Azure Firewall Premium is the right solution to protect your Azure virtual networks from malicious incoming and outgoing traffic.
- Evaluate whether Azure Firewall Manager is the right solution for deploying policies across multiple firewalls.
- Identify and describe use cases for Azure Firewall and Azure Firewall Manager.

Module 7: Guided Project - Configure secure access to workloads with Azure virtual networking services

In this module, you practice configuring secure access to workloads using Azure virtual networking. The lab combines both learning and hands-on practice.

Lessons

- Introduction.
- Exercise 01 - Create and configure virtual networks.
- Exercise 02 - Create and configure network security groups.
- Exercise 03 - Create and configure Azure Firewall.
- Exercise 04 - Configure network routing.
- Exercise 05 - DNS zones.
- Knowledge check.
- Summary and resources.

In this module, you'll practice how to:

-
- | | | |
|---|---|--|
| <ul style="list-style-type: none">– Create and configure virtual networks.– Create and configure network security groups (NSGs). | <ul style="list-style-type: none">– Create and configure Azure Firewall.– Configure network routing. | <ul style="list-style-type: none">– Create DNS zones and configure DNS settings. |
|---|---|--|

ASSOCIATED CERTIFICATIONS & EXAM

There is no Associated Certification or Exam for this course, however, there is an assessment to achieve your Applied Skills credential. ([Assessment Link](#))