

AZ-1002: Configure Secure Access to your Workloads Using Networking with Azure Virtual Network

Course Description

In this learning path, you practice configuring secure access to workloads using Azure networking.

Course Duration

1 day

Prerequisites

The prerequisites for the Microsoft AZ-1002 course, Configure Secure Access to your Workloads using Azure Virtual Networking, include:

- Basic knowledge of virtual networking in cloud environments.
- Familiarity with IP address formats and subnetting.
- Familiarity with Azure services, the Azure portal, and basic networking, DNS, and Azure Firewall concepts

Course Outline

- 1 - Configure virtual networks
 - Plan virtual networks
 - Create subnets
 - Create virtual networks
 - Plan IP addressing
 - Create public IP addressing
 - Associate public IP addresses
 - Allocate or assign private IP addresses
 - Module assessment
- 2 - Configure Azure Virtual Network peering
 - Determine Azure Virtual Network peering uses
 - Determine gateway transit and connectivity
 - Create virtual network peering
 - Extend peering with user-defined routes and service chaining
 - Module assessment
- 3 - Manage and control traffic flow in your Azure deployment with routes
 - Identify routing capabilities of an Azure virtual network
 - What is an NVA?
- 4 - Host your domain on Azure DNS
 - What is Azure DNS?
 - Configure Azure DNS to host your domain
 - Dynamically resolve resource name by using alias record

- 5 - Configure network security groups
 - Implement network security groups
 - Determine network security group rules
 - Determine network security group effective rules
 - Create network security group rules
 - Implement application security groups
 - Module assessment

- 6 - Introduction to Azure Firewall
 - What is Azure Firewall?
 - How Azure Firewall works
 - When to use Azure Firewall
 - When to use Azure Firewall Premium
 - Module assessment

Who Should Attend

- Administrator
- Network Engineer