training code: AZ-1002 / ENG DL 1d / EN

Configure secure access to your workloads using networking with Azure Virtual Network

Purpose of the training

This training is intended for IT specialists who deal with secure access to workloads using an Azure virtual network and perform tasks on the Azure platform on a daily basis. The training bridges the gap between entry-level and associate-level skills, helping participants progress in a wide range of IT roles, including infrastructure and security roles for administrators and architects. The course is designed to practice configuring and securing network resources, including creating and configuring virtual networks, network routing, DNS zones, DNS settings, network security groups, and Azure Firewall.

Benefits of completing the training

Acquiring knowledge and skills in the configuration and management of Azure virtual networks, including:

- Creating and configuring virtual networks.
- Network routing.
- DNS zones.
- DNS settings.
- Network security groups.
- Azure Firewall.

Expected Listener Preparation

- Experience using the Azure portal to create resources.

- Basic knowledge of enterprise networking and cloud networking concepts.
- Basic knowledge of network security concepts like firewalls, routing, and access control lists..

Training Language

- **Training**: English
- **Materials**: English

Training Includes

- manual in electronic form available on the platform:
- https://learn.microsoft.com/pl-pl/training/
- access to Altkom Akademia's student portal

Duration

1 days / 7 hours

Training agenda

1. Configure virtual networks.
   - Plan virtual networks.
   - Create virtual networks.
   - Create subnets.
   - Plan IP addressing.
   - Create public IP addressing.
   - Associate public IP addresses.
   - Allocate or assign private IP addresses.
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.

3. Manage and control traffic flow in your Azure deployment with routes.
   - Identify routing capabilities of an Azure virtual network.
   - Network virtual appliance (NVA).
4. Host your domain on Azure DNS.
   - Azure DNS.
   - Configure Azure DNS to host your domain.
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.
6. Introduction to Azure Firewall.
   - Azure Firewall.
   - How Azure Firewall works.
   - When to use Azure Firewall.
   - When to use Azure Firewall Premium.
7. Guided Project – Configure secure access to workloads with Azure virtual networking services.
   - Exercise – Provide network isolation and segmentation for the web application.
   - Exercise – Control the network traffic to and from the web application.
   - Exercise – Protect the web application from malicious traffic and block unauthorized access.
   - Exercise – Operationalize and enforce policy to filter traffic.
   - Exercise – Record and resolve domain names internally.