

Configure secure access to your workloads using Azure virtual networking (AZ-1002)

Duration: 1 day

Audience: Professionnel TI

Who is this training for?

- Intermediary
- Administrator
- Network Engineer
- Azure Firewall Manager

Training objectives

Upon completion of this course, participants will be able to:

- Configure Azure Virtual Networks (VNETs) and their segmentation (subnets, IP addressing)
- Set up connections between networks (peering) to ensure secure communication Control network traffic using custom routes and Azure routing
- Manage name resolution with Azure DNS (DNS zones, [learn.microsoft.com])
- Secure communications by configuring Network Security Groups (NSGs) and their rules
- Protect resources with Azure Firewall and its security policies Implement secure access to workloads through a full scenario (guided project)

Summary

Applied Skills training courses are designed to validate specific skills by being oriented towards real-world scenarios. They offer a targeted alternative to traditional role-based certifications, with a focus on applying technical skills in real-world business situations. In this training lab, you'll practice setting up secure access to workloads using the Azure network.

Course outline

- Configure virtual networks
- Configure Azure virtual network peering

- Manage and control the flow of traffic in your Azure deployment with routes
- Host your domain on Azure DNS
- Configure network security groups
- Introduction to Azure Firewall
- Guided project - Configure secure access to workloads with Azure virtual network services
- Explore the other Applied Skills: Microsoft applied skills (afiexpertise.com)

Approach and methodology

Practical and structured approach combining focused theory and guided workshops. Participants gradually set up secure access to workloads using the Azure virtual network through real-world exercises inspired by real-world scenarios, promoting immediate application of learnings. They learn how to design secure network architectures, manage access, and protect resources in the cloud. Led by a Microsoft certified trainer, the training focuses on interactivity and the development of directly transferable technical skills to effectively secure Azure environments in a professional context.

Prerequisites

You need an Azure subscription to complete these exercises. If you don't have an Azure subscription, create a free account and add a subscription before you begin. If you're a student, you can take advantage of the Azure for Students offer.

Recommendations

- Basics in networking (IP, DNS, subnets, routing)
- Knowledge of network security concepts (firewall, segmentation, secure access)
- Familiarity with Microsoft Azure" Notions of identity and access management (Entra ID)
- Understanding of cloud architectures