Microsoft Azure Security Technologies (AZ-500T00)

Duration: 4 days
Audience: Professionnel TI

Who is this training for?

Students should have at least one year of hands-on experience securing Azure workloads and experience with security controls for workloads on Azure.

Training objectives

- Describe specialized data classifications on Azure
- Identify Azure data protection mechanisms
- Use Azure data encryption methods
- Secure Internet protocols and how to integrate them on Azure
- Describe Azure security services and features

Summary

In this course, students will gain the knowledge and skills to implement security controls, maintain security posture, and identify and remediate vulnerabilities using a variety of security tools. The course covers scripting and automation, virtualization, and N-tier cloud architecture.

Course outline

Learning Path 1: Secure Identity and Access

- Manage Security Controls for Identity and Access
- Manage Access to Microsoft Entra Applications

Learning Path 2: Secure Networks

- Plan and Implement Security for Virtual Networks
- Plan and Implement Security for Private Access to Azure Resources
- Plan and Implement Security for Public Access to Azure Resources

Learning Path 3: Secure compute, storage, and databases

- Plan and implement advanced security for compute
- Plan and implement security for storage
- Plan and implement security for Azure SQL Database and Azure SQL Managed Instance
- Learning path 4: Manage Azure security with Microsoft Defender for Cloud and Microsoft Sentinel
- Implement and manage cloud governance policy enforcement
- Manage security posture with Microsoft Defender for Cloud
- Configure and manage threat protection with Microsoft Defender for Cloud
- Configure and manage security monitoring and automation solutions

Approach and methodology

Practical and structured approach combining focused theory and guided workshops. Participants progressively secure Azure environments using Microsoft Azure security technologies through real-world exercises inspired by professional scenarios, promoting immediate application of learnings. They learn how to protect identities, data, and assets, as well as how to implement the right security and governance controls. Led by a Microsoft certified trainer, the training focuses on interactivity and the development of directly transferable technical skills to strengthen the security posture of Azure environments in a professional context.

Prerequisites

Before taking this course, students should have knowledge of: Microsoft Azure Associate Administrator or equivalent content

Recommendations

- Basics of Azure administration Knowledge of cybersecurity concepts (threats, access control, encryption)
- Understanding of networks (IP, firewall, segmentation)
- Notions of identity management (Microsoft Entra ID)
-

Familiarity with Azure resources (VMs, storage, applications)