+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 01/08/2026

Register

Microsoft Azure AZ-5OO Certification Preparation Training

ALL-IN-ONE: EXAM INCLUDED IN THE PRICE

4 days (28 hours)

Presentation

Master securing workloads on Microsoft Azure with AZ-500 preparation. Learn how to reduce attack surfaces, automate controls, and meet compliance requirements. Ideal for protecting your applications, data, and identities in hybrid and cloud-native environments. By the end of this training, you will know how to design a Zero Trust architecture, implement conditional access, RBAC, and PIM, segment the network with NSG/ASG and Azure Firewall, protect data with Key Vault and encryption, and harden your posture with Azure Policy. The training focuses on guided workshops, reproducible labs, and step-by-step demos. IaaS, PaaS, and container use cases reinforce each skill.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Assess risks and define a Zero Trust strategy on Azure.
- Implement and harden identity and access (MFA, conditional access, RBAC, PIM).
- Secure networks and workloads (NSG/ASG, Azure Firewall, WAF).
- Protect secrets and data (Key Vault, encryption, SAS).
- Monitor, detect, and respond to threats (Defender for Cloud, Sentinel, Log Analytics).

Target audience

- Cloud/DevOps engineers
- System and security administrators

- Cloud architects

Prerequisites

- Azure basics (resources, resource groups, VNet, Storage).
- Network security and IAM concepts.
- Practical experience with PowerShell or Azure CLI.
- Technical English reading skills.

Technical prerequisites

- 64-bit computer with 8–16 GB of RAM.
- Windows 10/11, macOS, or Linux.
- Stable internet access and modern browser.
- Azure account with Contributor role (or sandbox provided during the session).
- Installed tools: Visual Studio Code, Azure CLI, PowerShell (Az module).

Our Microsoft Azure AZ-5OO training program

[Day 1 - Morning]

Fundamentals of Azure security and Zero Trust

- Shared responsibility, Zero Trust principles, and risk mapping
- Measuring posture with Microsoft Defender for Cloud and Secure Score
- Security governance: RBAC, tags, Azure Policy (initiatives, remediation)
- Best practices for segmentation, private access, and attack surface reduction
- Hands-on workshop: Express audit of a subscription and prioritized action plan

[Day 1 - Afternoon]

Identities and access control with Microsoft Entra ID (Azure AD)

- Entra ID roles vs. Azure RBAC: scopes, best practices for delegation
- Conditional access, MFA, session hardening, and basic protections
- PIM (Just-In-Time) for privileged roles and groups
- Service accounts and managed identities for resource access
- Hands-on workshop: Configuring PIM and a conditional access strategy

[Day 2 - Morning]

Network protection and segmentation

- VNet design, subnets, peering, and routing (UDR)
- Controls: NSG/ASG, Azure Firewall (DNAT/SNAT, application rules)
- Secure exposure: Private Link/Endpoints, Private DNS, Service Endpoints
- Perimeter: WAF (Application Gateway) and DDoS Protection
- Hands-on workshop: Segmenting a VNet and publishing an app via WAF and Private Link

[Day 2 - Afternoon]

Securing the platform layer: VMs, PaaS, and containers

- Hardening VMs: Update Management, Guest Configuration, disk encryption
- Secure PaaS: App Service/Functions (IP restrictions, VNet integration, Managed Identity)
- Container security: AKS, ACR, image scanning, and Defender for Containers
- Backup, resource locks, and restore as a safety net
- Hands-on workshop: Enabling Defender, scanning ACR images, and blocking non-compliant deployments

[Day 3 - Morning]

Log collection, KQL, and alerting

- Sources: Activity Log, Diagnostic Settings, and Log Analytics tables
- Ingestion with Data Collection Rules and workspace separation
- KQL queries for search, aggregations, and visualizations
- Alerts, Action Groups, and automation with Logic Apps
- Hands-on workshop: Create a dashboard and security-focused KQL alerts

[Day 3 - Afternoon]

Detection and response with Microsoft Sentinel

- Deploying Sentinel and data connectors (Azure, M365, Syslog)
- Analytics rules, correlation, and incident management
- SOAR automation: Logic Apps playbooks and guided responses
- Hunting: KQL queries, abnormal signals, and investigation best practices
- Hands-on workshop: Investigating an incident and automating a response

[Day 4 - Morning]

Data protection, keys, and secrets

- Encryption at rest/in transit: SSE with CMK, Azure Disk Encryption
- Key Vault: RBAC vs. policies, firewall/private network, soft delete, and purge protection
- Storage security: RBAC, shared keys, SAS, immutability (Blob)
- Secretless access with Managed Identities for apps and workloads
- Hands-on workshop: Deploy a Key Vault, rotate a secret, and link an app via Managed Identity

[Day 4 - Afternoon]

Application security and exam preparation

- App Service/Functions: Integrated AuthN/AuthZ, network restrictions, secrets
- DevSecOps: code/dependency scans, secrets scanning, and security gates in CI/CD
- Continuous compliance: Azure Policy (deny, DeployIfNotExists), assessment, and remediation
- Final review: skill areas, common pitfalls, and study plan

Mock exam

Target companies

This training is intended for both individuals and companies, large or small, wishing to train their teams in new advanced IT technologies or to acquire specific business knowledge or modern methods.

Placement at the start of training

The positioning at the start of the training complies with Qualiopi quality criteria. Upon final registration, the learner receives a self-assessment questionnaire that allows us to assess their estimated level of proficiency in different types of technologies, as well as their expectations and personal objectives for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could be problematic for the monitoring and smooth running of the training session.

Teaching methods

Practical training: 60% practical, 40% theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and discussion sessions, and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been correctly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training course.