

Azure For Developers

Training Outline

For .NET / Java / PHP / Python and other application developers

This training is designed for **beginner and intermediate-level developers** and starts from the basics before gradually moving toward building, securing, monitoring and designing real-world applications on Microsoft Azure.

The hands-on demos are primarily shown using **.NET and Visual Studio**. However, developers using **Java, PHP, Python or other programming languages** can easily follow the training because the core Azure concepts, services, security and architecture patterns remain the same.

01 Azure Fundamentals & Access Control

Build a strong Azure foundation before moving to application services.

- Azure account setup guidance, Tenant, Microsoft Entra ID and Subscriptions
- Tenant-level roles and Azure RBAC (Role-Based Access Control)
- IaaS, PaaS and SaaS in simple terms
- Regions, Data Centers, Availability Zones and Availability Sets
- Managed Identity and Service Principal concepts

02 Networking From Scratch

Learn the networking basics every cloud developer should understand.

- Public IP vs Private IP; IP Address and Port basics
- TCP, HTTP, HTTPS and RDP - what each one means
- Virtual Networks (VNET), Subnets and CIDR notation
- Create a Virtual Machine and understand NIC/Public IP
- Network Security Groups (NSG) and basic secure network design

03 Azure App Service & Host a Web App

Learn how web applications and APIs are hosted and managed in Azure App Service.

- Azure App Service and App Service Plan concepts
- Host an ASP.NET Core Web API / web application in Azure
- Environment Variables / application configuration
- Deployment Slots and scaling
- Azure Bastion overview and Private Endpoint introduction

04 Authentication, Authorization & OAuth 2.0

Understand how users sign in and how a secured backend API controls access.

- Authentication vs Authorization and why OAuth 2.0 is used
- Microsoft Entra ID App Registration, API permissions and exposed API scopes
- Protect an API and test OAuth 2.0 using Postman
- UI application calling an authenticated Backend API
- Access Tokens, role-based authorization and User vs Service-to-Service authentication

05 Azure Key Vault & Application Security

Keep secrets out of source code and understand secure application access patterns.

- Azure Key Vault fundamentals - Keys vs Secrets
- Secret/key expiry and secret rotation concepts
- Use Managed Identity to access Azure resources securely
- Key Vault with Private Endpoint and secure network access
- Practical Key Vault implementation and best-practice discussion

06 Monitoring, Logging, Metrics & Alerts

Learn how to understand application health and troubleshoot issues after deployment.

- Azure Monitor and Application Insights
- Application Insights in ASP.NET Core and custom application logs
- Important App Service, Azure SQL and Application Gateway metrics
- Alerts for HTTP 5xx errors, response time, CPU, failed connections and more
- Azure Dashboards for day-to-day monitoring

07 Private Networking for Web Applications

Move from a public application toward a secure real-world network design.

- Private Endpoint and VNET Integration - understand the difference
- Private DNS Zone concept
- Make the Backend API private instead of publicly accessible
- Allow the UI application to communicate securely with the Backend API
- Secure network designs for apps hosted in VM and Azure App Service

08 Azure Cache for Redis

Improve application performance by caching frequently used data.

- What Redis Cache is and when caching helps
- Connect an ASP.NET Core application to Azure Redis
- Use IDistributedCache to store and read cached values
- Serialize and deserialize .NET objects in cache
- When to use Redis, when not to use it and what to monitor

09 Azure Functions

Understand where serverless functions fit in an application.

- What Azure Functions are and when to use them
- When not to use Functions and Azure Functions vs ASP.NET Core Web API
- Event-driven and scheduled tasks in a real-world application

10 Azure API Management (APIM)

Understand when a centralized API layer becomes useful.

- What APIM is, when to use it and when it may be unnecessary
- Centralized API security, rate limiting and hiding backend URLs
- API analytics and exposing multiple backend APIs through one endpoint

11 Azure Application Gateway & WAF

Put a secure entry point in front of your web application.

- Application Gateway - what it is and why we use it
- Backend Pools, Listeners, Backend Settings and Health Probes
- Web Application Firewall (WAF) and WAF Policies
- Configure Application Gateway with Azure App Service
- Access the application through Application Gateway and block direct public access

12 Real-World Architecture & Developer Concepts

Connect individual Azure services together and understand how they fit into an actual application.

- Secure web application architecture with UI, Backend API and Azure SQL
- App Service, Private Endpoints, VNET Integration and Application Gateway working together
- Simple CI/CD roadmap for a .NET developer
- Production troubleshooting using logs, metrics, alerts and dashboards

13 Interview Preparation for Experienced Developers

Revise the same concepts through practical project and interview questions.

- Tenant vs Subscription, RBAC, networking, NSG and secure design
- Key Vault, Private Endpoint, Redis Cache and OAuth 2.0 scenarios
- Azure App Service, Deployment Slots and production troubleshooting
- Secure frontend-to-backend communication
- Azure Functions vs ASP.NET Core Web API - choosing the right option

Training approach: Start from scratch -> understand the concept -> see practical examples -> connect the service to a real-world application. The focus is on understanding why and where an Azure service is used, rather than simply memorizing features.