Implement Azure Security

AZ-203T04; 1 Day; Instructor-led

About This Course

In this course students will gain the knowledge and skills needed to include Azure authentication and authorization services in their development solutions. Students will learn how identity is managed and utilized in Azure solutions by using the Microsoft identity platform. Students will also learn about access control (claims-based authorization and role-based access control) and how to implement secure data solutions. Throughout the course students learn how to create and integrate these resources by using the Azure CLI, REST, and application code.

Audience

This course is intended for…

- Students interested in Azure development or in passing the Microsoft Azure Developer Associate certification exam.

Prerequisites

Before attending this course, students should have:

- 1-2 years of experience as a developer. This course assumes students know how to code and have a fundamental knowledge of Azure.
- It is recommended that students have some experience with PowerShell or Azure CLI, working in the Azure portal, and with at least one Azure-supported programming language. Most of the examples in this course are presented in C\# .NET.

Course Outline

Module 1: Implement authentication

Microsoft identity platform is an evolution of the Azure Active Directory (Azure AD) identity service and developer platform. It allows developers to build applications that sign in all Microsoft identities, get tokens to call Microsoft Graph, other Microsoft APIs, or APIs that developers have built.

Lessons

- Microsoft identity platform
- Implement OAuth2 authentication
- Implement managed identities for Azure resources
- Implement authentication by using certificates, forms-based authentication, or tokens
- Implement multi-factor authentication

After completing this module, students will be able to:

- Understand the architecture of the Microsoft identity platform
- Be able to implement OAuth2 authentication in their solutions
- Be able to use Azure Key Vault to store and retrieve authentication information

Module 2: Implement access control

This module covers claims-based and role-based access control.

Lessons

- Claims-based authorization
- Role-based access control (RBAC) authorization

After completing this module, students will be able to:

- Learn how to use claims-based authorization in their development solutions
- How to manage access to resources using RBAC through the REST API

Module 3: Implement secure data solutions

This module covers securing data at rest and during transmission.

Lessons

- Encryption options
- End-to-end encryption
- Implement Azure confidential computing
- Manage cryptographic keys in Azure Key Vault

After completing this module, students will be able to:

- Understand encryption options
- Learn how to encrypt data with Transparent Data Encryption
- Manage and utilize encryption keys by using the Azure key Vault