Implementing Authentication And Secure Data (AZ-300.5)

Modality: On Demand

Duration: 12 Hours

"The exam associated with this training has been retired. However for purely educational purposes you can access this training."

This course prepares you for the AZ-300 Exam leading to AZ-300 Certification. This course does not include the Official Exam Voucher, however, you can request to purchase the Official Exam Voucher separately.

About this course:

Learn how to Implement authentication in applications (certificates, Azure AD, Azure AD Connect, token-based), implement secure data (SSL and TLS), and manage cryptographic keys in Azure Key Vault.

Course Objective:

After completing this course, students will be able to:

- Understand how to Implement authentication using certificates, Azure AD, Azure AD Connect, and tokens.
- Implement Role-aBsed Access Control (RBAC) authorization.
- Implement secure data for end-to-end encryption.
- Implement secure data for implementing SSL and TLS communications.
- Use Azure Key Vault to manage cryptographic keys.

Audience:

- Successful Cloud Solutions Architects begin this role with practical experience with operating systems, virtualization, cloud infrastructure, storage structures, billing, and networking.

Prerequisite:

- practical experience with operating systems, virtualization, cloud infrastructure, storage structures, billing, and networking.

Course Outline:

Module 1 - Implementing Authentication

- Implementing authentication in applications

- Implement multi-facr authentication
- Claims-based authorization
- Role-based access control (RBAC) authorization
- Review Questions
- Module 1 Assessment

Module 2 - Implementing Secure Data

- Encryption options
- End--end encryption
- Implement Azure confidential computing
- Implement SSL and TLS communications
- Manage crypgraphic keys in Azure Key Vault
- Review Questions
- Module 2 Assessment