training code: AZ-1003 / ENG DL 1d / EN

Secure storage for Azure Files and Azure Blob Storage

Purpose of the training

Training intended for IT specialists who in their daily work are responsible for tasks related to secure data storage on the Azure platform. The training bridges the gap between entry-level and associate-level skills, enabling participants to achieve the specific knowledge required for many IT roles, including infrastructure, security and networking tasks. This course is designed to practice configuring and securing storage, including skills in creating and configuring storage accounts, blob containers, file shares, storage networking, and storage security.

Benefits of completing the training

Acquiring knowledge and skills in configuring and managing Azure storage, including:

- Create and configure storage accounts.
- Create and configure blob containers.
- Create and configure file shares.
- Creating and configuring a storage network.
- Create and configure storage security.

Expected Listener Preparation

- Experience using the Azure portal to create resources.
- Basic knowledge of unstructured data like blobs and files.
- Basic knowledge of security concepts like identities, permissions, and encryption.
- Basic knowledge of networking concepts like virtual networks and subnetting.

Training Language

- **Training**: English
- **Materials**: English

Training Includes

- manual in electronic form available on the platform:
- https://learn.microsoft.com/pl-pl/training/
- access to Altkom Akademia's student portal

Duration

1 days / 7 hours

Training agenda

1. Create an Azure Storage account.
    - Decide how many storage accounts you need.
    - Choose your account settings.
    - Choose an account creation tool.
2. Configure Azure Blob Storage.
    - Implement Azure Blob Storage.
    - Create blob containers.
    - Assign blob access tiers.
    - Add blob lifecycle management rules.
    - Determine blob object replication.
    - Upload blobs.
    - Determine Blob Storage pricing.
3. Configure Azure Storage security.
    - Review Azure Storage security strategies.
    - Create shared access signatures.

- Identify URI and SAS parameters.
- Determine Azure Storage encryption.
- Create customer-managed keys.
- Apply Azure Storage security best practices.

4. Secure and isolate access to Azure resources by using network security groups and service endpoints.
   - Use network security groups to control network access.
   - Secure network access to PaaS services with virtual network service endpoints.
5. Guided Project – Azure Files and Azure Blobs.
   - Exercise – Provide storage for the IT department testing and training.
   - Exercise – Provide storage for the public website.
   - Exercise – Provide private storage for internal company documents.
   - Exercise – Provide shared file storage for the company offices.
   - Exercise – Provide storage for a new company app.