AZ 1003- Secure Storage For Azure Files and Azure Blob Storage

Days: 1

Prerequisites: 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.

Description: In this learning path, you practice storing business data securely by using Azure Blob Storage and Azure Files. The skills validated include creating storage accounts, storage containers, and file shares. Also, configuring encryption and networking to improve the security posture.

OUTLINE:

LESSON 1 - CREATE AN AZURE STORAGE ACCOUNT

- Decide how many storage accounts you need
- Choose your account settings
- Choose an account creation tool
- Module assessment

LESSON 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
- Manage blobs
- Determine Blob Storage pricing
- Module assessment

LESSON 3 - CONFIGURE AZURE FILES

- Compare storage for file shares and blob data
- Manage Azure file shares
- Create file share snapshots
- Implement soft delete for Azure Files
- Use Azure Storage Explorer
- Consider Azure File Sync

LESSON 4 - 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
- Module assessment

LESSON 5 - 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

LESSON 6 - GUIDED PROJECT - AZURE FILES AND AZURE BLOBS

- Module assessment