KOENIG
step forward

AZ-1003: Secure storage for Azure Files and Azure Blob Storage

Create an Azure Storage account

Introduction

Decide how many storage accounts you need

Choose your account settings

Choose an account creation tool

Exercise - Create a storage account using the Azure portal

Knowledge check - Create a storage account

Summary

Configure Azure Blob Storage

Introduction

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

Interactive lab simulation

Knowledge check

Summary and resources

Configure Azure Storage security

Introduction

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

Interactive lab simulation

Knowledge check

Summary and resources

Secure and isolate access to Azure resources by using network security groups and service endpoints

Introduction

Use network security groups to control network access

Exercise - Create and manage network security groups

Secure network access to PaaS services with virtual network service endpoints

Exercise - Restrict access to Azure Storage by using service endpoints

Summary

Guided Project - Azure Files and Azure Blobs

Introduction

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

Knowledge check

Summary and resources