

**Secure Storage for Azure Files and Azure Blob Storage (AZ-1003)**

**Course Number:** MOC-AZ-1003  
**Duration:** 1 day

**Overview**

This Azure learning path, Secure Storage for Azure Files and Azure Blob Storage (AZ-1003), teaches attendees how to store business data securely by using Azure Blob Storage and Azure Files. Students learn how to create storage accounts, storage containers, and file shares. This Azure course also covers configuring encryption and networking to improve security.

**Prerequisites**

All AZ-1003 training students must have experience using the Azure portal to create resources and have basic knowledge of:

* Unstructured data like blobs and files
* Security concepts like identities, permissions, and encryption
* Networking concepts like virtual networks and subnetting

**Materials**

All Microsoft Azure training students receive Microsoft official courseware.

For all Microsoft Official Courses taught in their entirety that have a corresponding certification exam, an exam voucher is included for each participant.

**Software Needed on Each Student PC**

Students need an Azure subscription to complete these exercises. If they don't have an Azure subscription, they may create a [free account](https://azure.microsoft.com/free/?azure-portal=true) and add a subscription before the class.

**Objectives**

* Create an Azure Storage account with the correct options for your business needs
* Configure Azure Blob Storage, including tiers and object replication
* Configure common Azure Storage security features like storage access signatures
* Use network security groups and service endpoints help secure virtual machines and Azure services from unauthorized network access
* Practice storing business data securely by using Azure Blob Storage and Azure Files

**Outline**

* Create an Azure Storage account
  + 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
* 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
  + Interactive lab simulation
* 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
  + Interactive lab simulation
  + Secure and isolate access to Azure resources by using network security groups and service endpoints
  + 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
* 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