MS-AZ1003: SECURE STORAGE FOR AZURE FILES AND AZURE BLOB STORAGE

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
1 Day	Intermediate	Azure	Instructor-led	NA

INTRODUCTION

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.

AUDIENCE PROFILE

This course is designed for IT professionals who are responsible for securing data stored in Azure, which includes:

- Azure Administrators: Individuals who manage Azure storage solutions must ensure data security.
- Cloud Administrators: Professionals overseeing cloud infrastructure and services, focusing on secure storage practices.
- IT Professionals: Those with roles in infrastructure, security, and networking who are looking to enhance their skills in Azure storage security.

PREREQUISITES

Before attending this course, delegates must have:

- 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.

COURSE OBJECTIVES

After completing this course, students will be able to:

- Create and Configure Storage Accounts: Learn how to set up and manage Azure storage accounts.
- Create and Configure Blob Storage: Understand how to create and manage blob containers and objects.
- Create and Configure Azure Files: Gain skills in setting up and managing Azure file shares.
- Configure Networking for Storage: Learn to configure network settings to secure storage access.

COURSE CONTENT

Module 1: Create an Azure Storage account

Create an Azure Storage account with the correct options for your business needs.

Learning objectives

- 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.

By the end of this module, you'll be able to:

- Decide how many storage accounts you need for your project.
- Determine the appropriate settings for each storage account.
- Create a storage account using the Azure portal.

Module 2: Configure Azure Blob Storage

Azure Virtual Desktop design requires that you assess network capacity and speed requirements, select a load-balancing method for your Azure Virtual Desktop deployment, and choose the right Windows Desktop client.

Learning objectives

- 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.

By the end of this module, you'll be able to:

- Configure a shared access signature (SAS), including the uniform resource identifier (URI) and SAS parameters.
- Configure Azure Storage encryption.
- Implement customer-managed keys.
- Recommend opportunities to improve Azure Storage security.

Module 3: Configure Azure Storage security

Your users require access to those applications both on-premises and in the cloud. You use the Remote Desktop client for Windows Desktop to access Windows apps and desktops remotely from a different Windows device.

Learning objectives

- 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.

By the end of this module, you'll be able to:

- Configure a shared access signature (SAS), including the uniform resource identifier (URI) and SAS parameters.
- Configure Azure Storage encryption.
- Implement customer-managed keys.
- Recommend opportunities to improve Azure Storage security.

Module 4: Implement storage security

See how to monitor and repair health of their Azure Virtual Desktop including virtual machines, virtual networks, application gateways, and load balancers.

Lessons

- Introduction.
- Implement Azure virtual network connectivity.
- Manage connectivity to the internet and on-premises networks.
- Understanding Azure Virtual Desktop network connectivity.
- Implement and manage network security for Azure Virtual Desktop.
- Configure Azure Virtual Desktop session hosts using Azure Bastion.
- Monitor and troubleshoot network connectivity for Azure Virtual Desktop.
- Plan and implement Remote Desktop Protocol Shortpath.
- Configure Remote Desktop Protocol Shortpath for managed networks.
- Configure Windows Defender Firewall with Advanced Security for RDP Shortpath.
- Plan and implement Quality of Service for Azure Virtual Desktop.
- Knowledge check.

By the end of this module, you'll be able to:

- Recommend a solution for Azure Virtual Desktop network connectivity.
- Implement Azure virtual network connectivity for Azure Virtual Desktop.
- Describe network security for Azure Virtual Desktop.
- Configure Azure Virtual Desktop session hosts using Microsoft Bastion.
- Monitor communication between a virtual machine and an endpoint.

Module 5: Secure and isolate access to Azure resources by using network security groups and service endpoints

Network security groups and service endpoints help you secure your virtual machines and Azure services from unauthorized network access.

Lessons

- 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.

In this module, you'll practice how to:

- Identify the capabilities and features of network security groups.
- Identify the capabilities and features of virtual network service endpoints.
- Use network security groups to restrict network connectivity.
- Use virtual network service endpoints to control network traffic to and from Azure services.

Module 6: Guided Project - Azure Files and Azure Blobs

In this module, you practice storing business data securely by using Azure Blob Storage and Azure Files. The lab combines both learning and hands-on practice.

Lessons

- 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 resource.

In this module, you'll practice how to:

- Create and configure a storage account.
- Create and configure blob storage.
- Create and configure Azure Files.
- Configure encryption for storage.
- Configure networking for storage.

ASSOCIATED CERTIFICATIONS & EXAM

There is no Associated certification & Exam for this course, however, there is an assessment to achieve your Applied Skills credential. (Assessment Link)