NETCAMPUS GROUP
unlocking potential

APPLIED SKILLS

Secure storage for Azure Files and Azure Blob Storage

Days	SKILL LEVEL	DELIVERY METHOD	Role	TECHNOLOGY
1	Intermediate	VILT/ILT	Administrator	Infrastructure

Course Overview

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.

Tasks performed.

- Create and configure a storage account
- Create and configure Blob Storage
- Create and configure Azure Files
- Configure encryption
- Configure networking for storage

Prerequisites

Before attending this course, delegates must know:

- Experience with the Azure portal
- Familiarity with the Azure data services Blobs, Files, Queues, and Tables
- Knowledge of basic networking concepts, including subnets and IP addressing
- Basic familiarity with Azure services, specifically Azure SQL Database and Azure Storage
- Familiarity with Azure virtual machines and virtual networking

Prepare for the assessment.

Module 1: Create an Azure Storage account

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

Learning objectives

In this module, you will:

- 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

Learn how to configure Configure Azure Blob Storage, including tiers and object replication.

Learning objectives

In this module, you learn how to:

- Understand the purpose and benefits of Azure Blob Storage.
- Create and configure Azure Blob Storage accounts.
- Manage containers and blobs within Azure Blob Storage.
- Optimize blob storage performance and scalability.
- Implement lifecycle management policies to automate data movement and deletion.
- Determine the best pricing plans for your Azure Blob Storage.

Module 3: Configure Azure Storage security

Learn how to configure common Azure Storage security features like storage access signatures.

Learning objectives

In this module, you learn how 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: 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.

Learning objectives

In this module, you will:

- 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 5: 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.

Learning objectives

In this module, you 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.

Take the assessment.

This assessment will use an interactive lab to evaluate your performance. It will take a few minutes to load the lab, and you may do other activities while it loads. After you launch the lab, you will need to wait 72 hours to launch it again. Your mouse movements and text entered during the lab will be recorded for quality purposes. Learn more.

Follow on Course

Schedules | Netcampus Group