

CANTON WEKE OTIENO

SECURITY ENGINEER TRACK

STUDENT TRACKING NUMBER; ADC-SE01-24010

CYBER SHUJAA

INSTRUCTOR: Dr. Paula

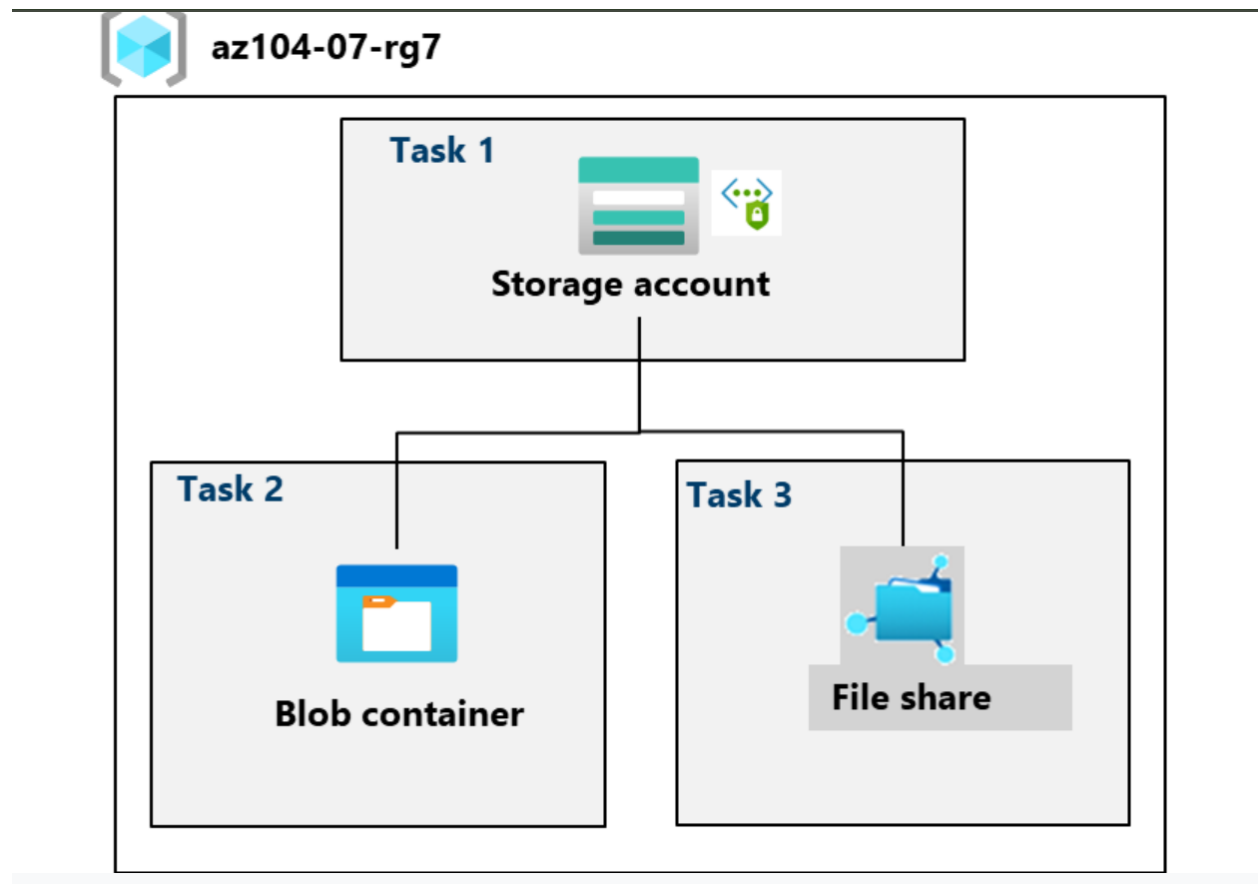
MANAGE AZURE STORAGE

Azure Storage provides a massively scalable object store. It offers a NoSQL database, a messaging store for dependable messaging, and a file system service for cloud computing. Azure Storage supports three categories of data, they include structured data, unstructured data, and finally virtual machine data. Azure Storage offers four data services that can be accessed by using an Azure storage account.

They include:

- **Azure Blob Storage (containers):** A massively scalable object store for text and binary data.
- **Azure Files:** Managed file shares for cloud or on-premises deployments.
- **Azure Queue Storage:** A messaging store for reliable messaging between application components.
- **Azure Table Storage:** A service that stores nonrelational structured data (also known as structured NoSQL data).

Architecture diagram



Introduction

This report contains instructions on to create storage accounts for Azure blobs and azure files, how to to configure and secure blob containers. And finally, the lab illustrates how to use Storage Browser to configure and secure Azure file shares. This lab prepare individual on how to manage azure storage in the real-world scenarios. It contains step on how to fully configure and mange azure storage.

Task 1: Create and configure a storage account.

In this lab one I created and configured a storage account. The storage account used geo-redundant storage with no public access.

Instructions

- Sign in to the Azure portal - <https://portal.azure.com>.
- Search for and select Storage accounts, and then click + Create.
- On the Basics tab of the Create a storage account blade, specify the following settings (leave others with their default values):

The screenshot shows the 'Create a storage account' blade in the Azure portal, specifically the 'Basics' tab. The page has a blue header with the Microsoft Azure logo, a search bar, and a Copilot button. Below the header, there's a breadcrumb trail: 'Home > Storage accounts >'. The main title is 'Create a storage account' followed by three dots. The form is divided into two sections: 'Project details' and 'Instance details'. In the 'Project details' section, there's a description: 'Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.' Below this, there are two dropdown menus: 'Subscription *' with 'Azure for Students' selected, and 'Resource group *' with '(New) az104-rg7' selected. A 'Create new' link is visible below the resource group dropdown. In the 'Instance details' section, there are three fields: 'Storage account name *' with 'bucket123' entered, 'Region *' with '(US) East US' selected, and 'Performance *' with 'Standard' selected. The 'Standard' option is described as 'Recommended for most scenarios (general-purpose v2 account)'. The 'Premium' option is described as 'Recommended for scenarios that require low latency.' At the bottom of the form, there are three buttons: 'Previous' (disabled), 'Next' (disabled), and 'Review + create' (active).

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > Storage accounts >

Create a storage account ...

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription * Azure for Students

Resource group * (New) az104-rg7
[Create new](#)

Instance details

Storage account name * ① bucket123

Region * ① (US) East US
[Deploy to an Azure Extended Zone](#)

Performance * ①

☒ **Standard:** Recommended for most scenarios (general-purpose v2 account)

☐ **Premium:** Recommended for scenarios that require low latency.

[Previous](#) [Next](#) [Review + create](#)

- On the Advanced tab, use the informational icons to learn more about the choices. Take the defaults.

Create a storage account ...

Basics Advanced Networking Data protection Encryption Tags Review + create

Security

Configure security settings that impact your storage account.

Require secure transfer for REST API operations ⓘ ☒

Allow enabling anonymous access on individual containers ⓘ ☐

Enable storage account key access ⓘ ☒

Default to Microsoft Entra authorization in the Azure portal ⓘ ☐

Minimum TLS version ⓘ

Version 1.2 ▾

Permitted scope for copy operations (preview) ⓘ

From any storage account ▾

Previous

Next

Review + create

- On the Networking tab, review the available options, select Disable public access and use private access.

Create a storage account ...

Basics Advanced Networking Data protection Encryption Tags Review + create

Network connectivity

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Network access *

- ☐ Enable public access from all networks
- ☐ Enable public access from selected virtual networks and IP addresses
- ☒ Disable public access and use private access

Private endpoint

Create a private endpoint to allow a private connection to this resource. Additional private endpoint connections can be created within the storage account or private link center.

[+ Add private endpoint](#)

Previous

Next

Review + create

- Review the Data protection tab. Notice 7 days is the default soft delete retention policy. Note you can enable blob versioning. Accept the defaults

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Storage accounts >

Create a storage account

BasicsAdvancedNetworkingData protectionEncryptionTagsReview + create

Recovery

Protect your data from accidental or erroneous deletion or modification.

☐

Enable point-in-time restore for containers

Use point-in-time restore to restore one or more containers to an earlier state. If point-in-time restore is enabled, then versioning, change feed, and blob soft delete must also be enabled. [Learn more](#)

☒

Enable soft delete for blobs

Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. [Learn more](#)

Days to retain deleted blobs

7

☒

Enable soft delete for containers

Soft delete enables you to recover containers that were previously marked for deletion. [Learn more](#)

Days to retain deleted containers

7

Previous

Next

Review + create

- Review the Encryption tab. Notice the additional security options. Accept the defaults.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Storage accounts >

Create a storage account

BasicsAdvancedNetworkingData protectionEncryptionTagsReview + create

Encryption type *

☒

Microsoft-managed keys (MMK)

☐

Customer-managed keys (CMK)

Enable support for customer-managed keys

☒

Blobs and files only

☐

All service types (blobs, files, tables, and queues)

This option cannot be changed after this storage account is created.

Enable infrastructure encryption

☐

- Select Review, wait for the validation process to complete, and then click Create.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with the Microsoft Azure logo, a search bar, and a Copilot button. Below the navigation bar, the breadcrumb path is 'Home > bucket123_1720086908443 | Overview'. The main content area displays a green checkmark and the message 'Your deployment is complete'. Below this, deployment details are listed: Deployment name: bucket123_172008690..., Subscription: Azure for Students, Resource group: az104-rg7, Start time: 7/4/2024, 12:55:51 PM, and Correlation ID: ce44d6c4-ab20-4220-afa4-3f99ff1c541a. A 'Go to resource' button is prominently displayed. On the right sidebar, there are links for 'Cost Manager', 'Microsoft Defender for Cloud', and 'Free Micro Start learni'.

- Once the storage account is deployed, select Go to resource.
- Review the Overview blade and the additional configurations that can be changed. These are global settings for the storage account. Notice the storage account can be used for Blob containers, File shares, Queues, and Tables.

The screenshot shows the 'Properties' tab of the 'bucket123' storage account in the Microsoft Azure portal. The left sidebar contains a navigation menu with options like Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Mover, Data storage, Security + networking, Data management, Settings, and Monitoring. The main content area is divided into three sections: Blob service, File service, and Security. The Blob service section lists various settings such as Hierarchical namespace (Disabled), Default access tier (Hot), Blob anonymous access (Disabled), Blob soft delete (Enabled (7 days)), Container soft delete (Enabled (7 days)), Versioning (Disabled), Change feed (Disabled), NFS v3 (Disabled), Allow cross-tenant replication (Disabled), and Storage tasks assignments (None). The File service section shows 'Large file share' as Enabled. The Security section lists 'Require secure transfer for REST API operations' (Enabled), 'Storage account key access' (Enabled), 'Minimum TLS version' (Version 1.2), and 'Infrastructure encryption' (Disabled). The Networking section shows 'Allow access from' (Selected networks), 'Number of private endpoint connections' (0), 'Network routing' (Microsoft network routing), 'Access for trusted Microsoft services' (Yes), and 'Endpoint type' (Standard).

In the Security + networking section, select Networking. Notice public network access is disabled.

- Change the public access level to Enabled from selected virtual networks and IP addresses.
- In the Firewall section, check the box for Add your client IP address.
- Be sure to Save your changes.

The screenshot shows the Microsoft Azure portal interface. At the top, the navigation bar includes the Microsoft Azure logo, a search bar, and the Copilot icon. The breadcrumb trail indicates the path: Home > bucket123_1720086908443 | Overview > bucket123. The main heading is 'bucket123 | Networking', with 'Storage account' noted below. A left-hand navigation pane lists various services, with 'Networking' selected under the 'Security + networking' category. The main content area is divided into three sections: 'Public network access', 'Virtual networks', and 'Firewall'. In the 'Public network access' section, the radio button for 'Enabled from selected virtual networks and IP addresses' is selected. The 'Virtual networks' section shows a table with columns for Virtual Network, Subnet, Address range, Endpoint Status, and Resource Group, but it currently displays 'No network selected.' The 'Firewall' section includes a link to 'Learn more' and a checked checkbox for 'Add your client IP address ('102.2.203.51')'. Below this, there is an 'Address range' section with a text input field labeled 'IP address or CIDR'.

Microsoft Azure Search resources, services, and docs (G+/)

Home > bucket123_1720086908443 | Overview > bucket123

bucket123 | Networking ☆ ...
Storage account

Search

Events

Storage browser

Storage Mover

> Data storage

Security + networking

Networking

Front Door and CDN

Access keys

Shared access signature

Encryption

Microsoft Defender for Cloud

> Data management

> Settings

Public network access

☐ Enabled from all networks

☒ Enabled from selected virtual networks and IP addresses

☐ Disabled

Configure network security for your storage accounts. [Learn more](#)

Virtual networks

+ Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group
No network selected.				

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. [Learn more](#).

☒ Add your client IP address ('102.2.203.51') ⓘ

Address range

IP address or CIDR

- In the Data management section, view the Redundancy blade. Notice the information about your primary and secondary data center locations.

Microsoft Azure | Search resources, services, and docs (G+)

Home > bucket123_1720086908443 | Overview > bucket123

bucket123 | Redundancy

Storage account

Search | Save | Discard | Prepare for failover | Refresh | Give feedback

> Data storage

✓ Security + networking

- Networking
- Front Door and CDN
- Access keys
- Shared access signature
- Encryption
- Microsoft Defender for Cloud

✓ Data management

- Storage tasks (preview)
- Redundancy**
- Data protection
- Object replication

Azure Storage redundancy copies your data so that it is protected from transient hardware failures, network or power outages, and natural disasters. If the primary endpoint becomes unavailable, then you can initiate a failover to the secondary endpoint to rapidly restore write access to your data. [Learn more about storage account failover](#)

Redundancy: Read-access geo-redundant storage (RA-GRS)

Last failover time: -

Storage endpoints: [View all](#)

Location	Data center type	Status	Failover
East US	Primary	Available	-
West US	Secondary	Available	-

- In the Data management section, select Lifecycle management, and then select Add a rule. Name the rule Movetocool. Notice your options for limiting the scope of the rule.

Microsoft Azure | Search resources, services, and docs (G+)

Home > bucket123_1720086908443 | Overview > bucket123 | Lifecycle management >

Add a rule

1 Details | 2 Base blobs

A rule is made up of one or more conditions and actions that apply to the entire storage account. Optionally, specify that rules will apply to particular blobs by limiting with filters.

Rule name *:

Rule scope *

☒ Apply rule to all blobs in your storage account

☐ Limit blobs with filters

Blob type *

☒ Block blobs

☐ Append blobs

Blob subtype *

☒ Base blobs

[Previous](#) [Next](#)

- On the Base blobs tab, if based blobs were last modified more than 30 days ago then move to cool storage. Notice your other choices.

Home > bucket123_1720086908443 | Overview > bucket123 | Lifecycle management >

Add a rule

Lifecycle management uses your rules to automatically move blobs to cooler tiers or to delete them. If you create multiple rules, the associated actions must be implemented in tier order (from hot to cool storage, then archive, then deletion).

If

Base blobs were *

☒ Last modified

☐ Created

More than (days ago) *

30

↓

Then

Move to cool storage

↓

+ Add conditions

Previous Add

- Notice you can configure other conditions. Select Add when you are done exploring.

Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

Home > bucket123_1720086908443 | Overview > bucket123

bucket123 | Lifecycle management

Storage account

Search

Encryption

Microsoft Defender for Cloud

Data management

Storage tasks (preview)

Redundancy

Data protection

Object replication

Blob inventory

Static website

Lifecycle management

Azure AI Search

Settings

Monitoring

+ Add a rule

✓ Enable

□ Disable

↻ Refresh

🗑 Delete

🗨 Give feedback

Lifecycle management offers a rich, rule-based policy for general purpose v2 and blob storage accounts. Use the policy to transition your data to tiers or expire at the end of the data's lifecycle. A new or updated policy may take up to 48 hours to complete. [Learn more](#)

List View

Code View

Enable access tracking ⓘ

□

□ Name	Status
Movetocool	Enabled

Task 2: Create and configure secure blob storage

In this lab two task, I created a blob container to help store unstructured data and uploaded an image.

Create a blob container and a time-based retention policy

- Continue in the Azure portal, working with your storage account.
- In the Data storage section, click Containers.
- Click + Container and Create a container with the following settings:

The screenshot displays the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and the Copilot icon. The breadcrumb trail shows the path: Home > bucket123_1720086908443 | Overview > bucket123. The main content area is titled 'bucket123 | Containers' and shows a 'Storage account' overview. On the left, a sidebar lists various services, with 'Containers' selected under the 'Data storage' section. The main area displays a table of containers with the following data:

Name	Last modified
\$logs	7/4/2024, 12:56:25 PM

Overlaid on the right is the 'New container' dialog box. It contains the following fields and options:

- Name ***: A text input field containing 'data'.
- Anonymous access level**: A dropdown menu set to 'Private (no anonymous access)'.
- Message**: A blue information icon followed by the text: 'The access level is set to private disabled on this storage account'.
- Advanced**: A collapsed section indicated by a downward arrow.
- Create**: A blue button at the bottom right of the dialog.

- On your container, scroll to the ellipsis (...) on the far right, select Access Policy.
- In the Immutable blob storage area, select Add policy.

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > buc

buc Storage

» + Co

Search

Immutable Storage policy

Policy type

Time-based retention

Set retention period for * ⓘ

180 ✓

days

☐ Enable version-level immutability ⓘ

i In order to enable version-level immutability support, your storage account must have versioning turned on.

Allow protected append writes to ⓘ

☒ None

☐ Append blobs

☐ Block and append blobs

Save Cancel

- Select Save.

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > bucket123_1720086908443 | Overview > bucket123

bucket123 | Containers Storage account

» + Container Change access level Restore containers Refresh ...

Search containers by prefix

☐ Show deleted containers

	Name	Last modified	Anonymous access l...	Lease state
<input type="checkbox"/>	\$logs	7/4/2024, 12:56:25 PM	Private	Available
<input checked="" type="checkbox"/>	data	7/4/2024, 1:26:59 PM	Private	Available

Manage blob uploads

- Return to the containers page, select your data container and then click Upload.
- On the Upload blob blade, expand the Advanced section.
- Confirm you have a new folder, and your file was uploaded.

Microsoft Azure Search resources, services, and docs (G+/) Copilot

Home > bucket123_1720086908443 | Overview > bucket123 | Containers >

data Container

Search Upload Change access level Refresh Delete

Authentication method: Access key (Switch to Microsoft Entra user account) Location: data

Search blobs by prefix (case-sensitive)

Add filter

No results

Upload blob

Drag and drop files here or [browse for files](#)

☐ Overwrite if files already exist

Advanced

Blob type

☒ Upload .vhd files as page blobs (recommended)

Block size

Access tier

Upload to folder

Blob index tags

Key	Value
-----	-------

- Confirm you have a new folder, and your file was uploaded.

Home > bucket123_1720086908443 | Overview > bucket123 | Containers >

data
Container

Overview

Diagnose and solve problems

Access Control (IAM)

Settings

Upload

Change access level

Refresh

...

Authentication method: Access key ([Switch to Microsoft Entra user account](#))
Location: data / securitytest

☐ Show deleted blobs

+ Add filter

Name	Modified	Access tier
<input type="checkbox"/> [..]		
<input type="checkbox"/> azuredeploydisk....	7/4/2024, 1:36:59 PM	Hot (Inferred)

- Select your upload file and review the options including Download, Delete, Change tier, and Acquire lease.

... > bucket123 | Containers > data >

securitytest/azuredeploydisk.bicep
Blob

Save

Discard

Download

Refresh

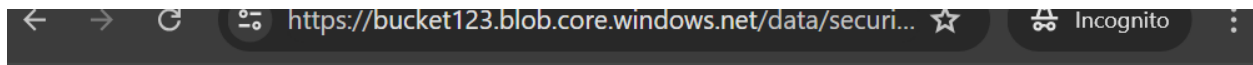
Delete

Change tier

...

LAST MODIFIED	7/4/2024, 1:36:59 PM
CREATION TIME	7/4/2024, 1:36:59 PM
VERSION ID	-
TYPE	Block blob
SIZE	854 B
ACCESS TIER	Hot (Inferred)
ACCESS TIER LAST MODIFIED	N/A
ARCHIVE STATUS	-
REHYDRATE PRIORITY	-
SERVER ENCRYPTED	true
ETAG	0x8DC9C153C462628
VERSION-LEVEL IMMUTABILITY POLICY	Disabled
CACHE-CONTROL	<input type="text"/>
CONTENT-TYPE	<input type="text" value="application/octet-stream"/>
CONTENT-MD5	<input type="text" value="cQL3PO400654GgYAIP7IIQ=="/>
CONTENT-ENCODING	<input type="text"/>

- Copy the file URL and paste into a new Inprivate browsing window.
- You should be presented with an XML-formatted message stating ResourceNotFound or PublicAccessNotPermitted.



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```

▼<Error>
  <Code>PublicAccessNotPermitted</Code>
  <Message>Public access is not permitted on this storage account. RequestId:bd422eab-d01e-0075-2100-cea3b3000000 Time:2024-07-04T10:56:08.7195342Z</Message>
</Error>

```

Configure limited access to the blob storage

- Select your uploaded file and then on the Generate SAS tab. You can also use the ellipsis (...) to the far right. Specify the following settings (leave others with their default values):

 A screenshot of the Microsoft Azure portal interface. The breadcrumb trail shows 'bucket123 | Containers > data > securitytest/azuredeploydisk.bicep'. The page title is 'securitytest/azuredeploydisk.bicep' with a 'Blob' subtitle. Action buttons include Save, Discard, Download, Refresh, and Delete. The 'Permissions' section has a dropdown set to 'Read'. The 'Start and expiry date/time' section includes fields for Start date (07/03/2024), Start time (2:02:28 PM), and a time zone dropdown (UTC+03:00) Nairobi. The 'Expiry' section includes fields for Expiry date (07/05/2024), Expiry time (10:02:28 PM), and a time zone dropdown (UTC+03:00) Nairobi. The 'Allowed IP addresses' field contains the text 'for example, 168.1.5.65 or 168.1.5.65-168.1....'. The 'Allowed protocols' section has radio buttons for 'HTTPS only' (selected) and 'HTTPS and HTTP'. At the bottom is a blue button labeled 'Generate SAS token and URL'.


- Click **Generate SAS token and URL**.

Allowed protocols ⓘ


☒ HTTPS only ☐ HTTPS and HTTP

Generate SAS token and URL

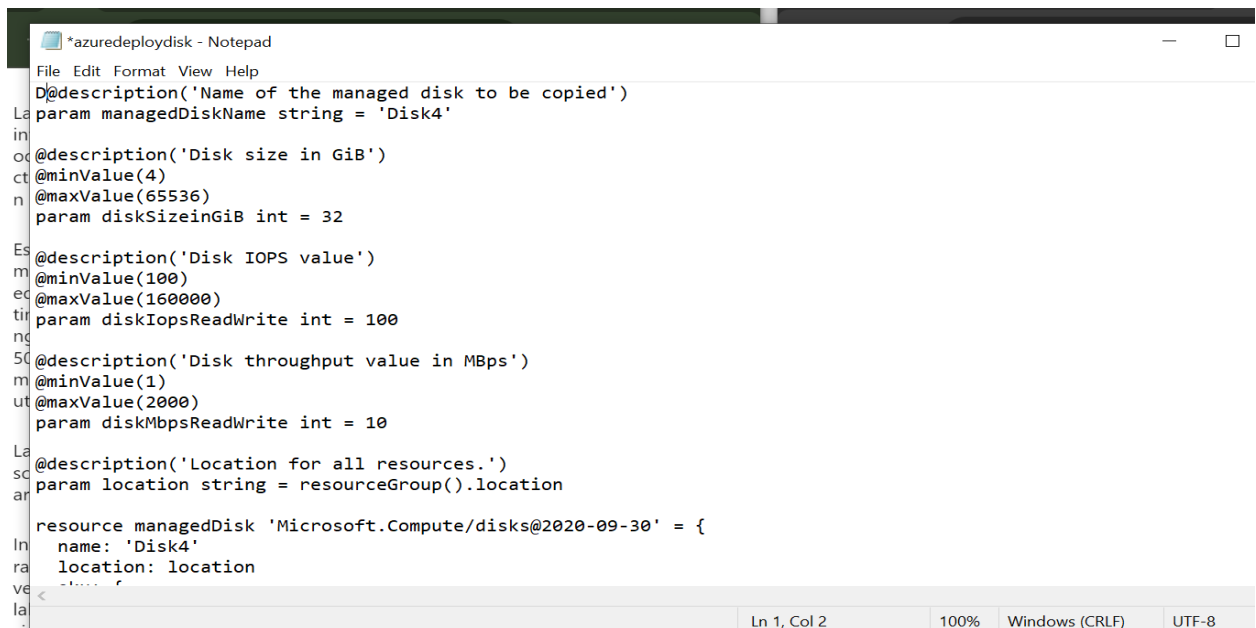
Blob SAS token ⓘ

sp=r&st=2024-07-03T11:02:28Z&se=2024-07-05T19:02:28Z&spr=https&sv=2022-11-02&sr=b&sig... 

Blob SAS URL

https://bucket123.blob.core.windows.net/data/securitytest/azuredeploydisk.bicep?sp=r&st=2024-07... 

- Copy the **Blob SAS URL** entry to the clipboard.
- Open another InPrivate browser window and navigate to the Blob SAS URL you copied in the previous step.



```
*azuredeploydisk - Notepad
File Edit Format View Help
@description('Name of the managed disk to be copied')
param managedDiskName string = 'Disk4'

@description('Disk size in GiB')
@minValue(4)
@maxValue(65536)
param diskSizeinGiB int = 32

@description('Disk IOPS value')
@minValue(100)
@maxValue(160000)
param diskIopsReadWrite int = 100

@description('Disk throughput value in MBps')
@minValue(1)
@maxValue(2000)
param diskMbpsReadWrite int = 10

@description('Location for all resources.')
param location string = resourceGroup().location

resource managedDisk 'Microsoft.Compute/disks@2020-09-30' = {
  name: 'Disk4'
  location: location
}
```

Ln 1, Col 2 100% Windows (CRLF) UTF-8

Task 3: Create and configure an Azure File storage.

In this task three I configured azure file share. Azure File Shares makes it easy for multiple users to share files and collaborate on projects

Instructions for creating File storage

- Create the file share and upload a file
- In the Azure portal, navigate back to your storage account, in the Data storage section, click File shares.
- Click + File share and on the Basics tab give the file share a name, share1.
- Notice the Access tier options. Keep the default Transaction optimized.
- Move to the Backup tab and ensure Enable backup is not checked. We are disabling backup to simplify the lab configuration.
- Click Review + create, and then Create. Wait for the file share to deploy.

Home > bucket123_1720086908443 | Overview > bucket123 | File shares >

New file share

Basics Backup Review + create

Azure Backup protects your file shares from accidental deletion or modification with granular restore and at-scale management capabilities. [Learn more](#)

Enable backup ☒

Recovery Services Vault ⓘ *

☒ Create new

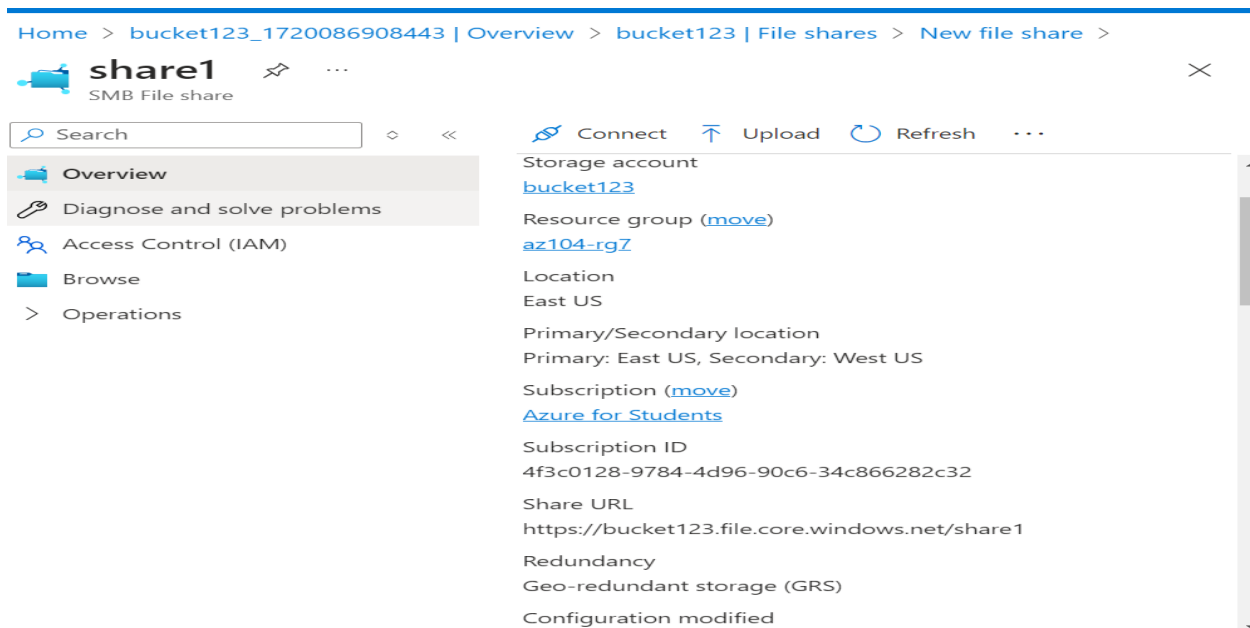
☐ Select existing

Vault name * vault-ly76gr38

Resource group * az104-rg7

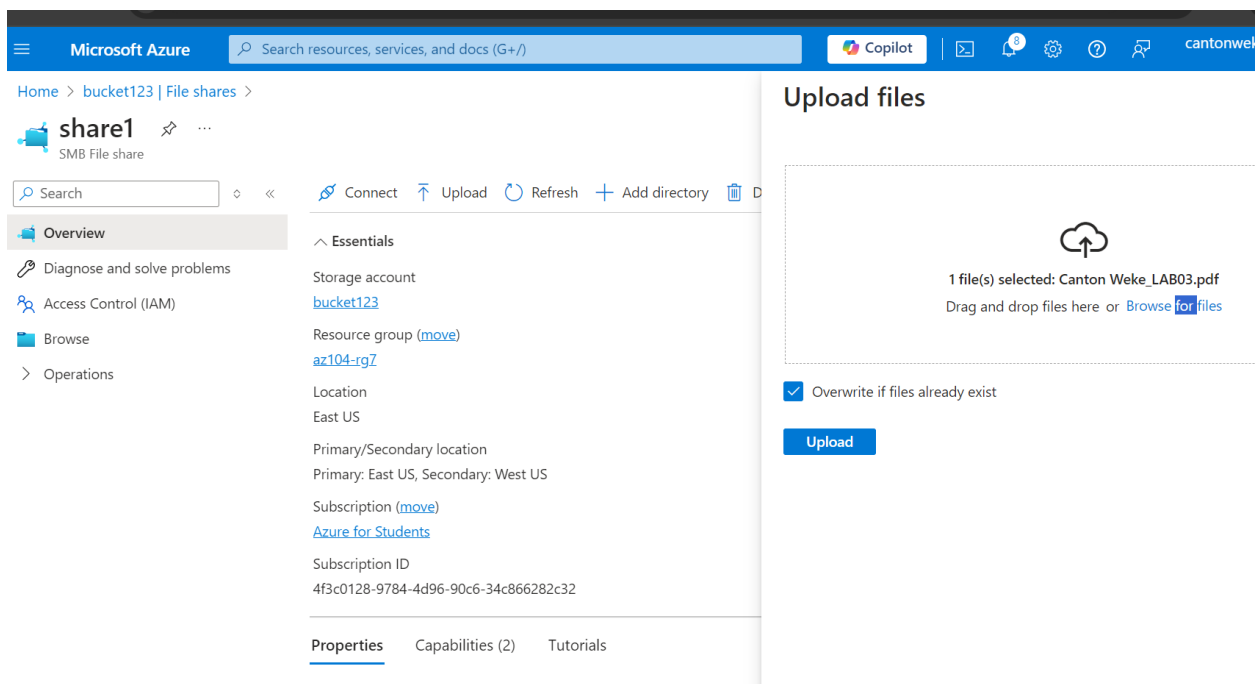
Backup policy * (new) DailyPolicy-ly76grif

[Edit this policy](#)



Explore Storage Browser and upload a file

- Return to your storage account and select **Storage browser**. The Azure Storage Browser is a portal tool that lets you quickly view all the storage services under your account.
- Select **File shares** and verify your **share1** directory is present.
- Select your **share1** directory and notice you can + **Add directory**. This lets you create a folder structure.
- Select **Upload**. Browse to a file of your choice, and then click **Upload**.



Restrict network access to the storage account

- In the portal, search for and select Virtual networks.
- Select + Create. Select your resource group. and give the virtual network a name, vnet1.
- Take the defaults for other parameters, select Review + create, and then Create.

[Home](#) > [Virtual networks](#) >

Create virtual network

Basics Security IP addresses Tags Review + create

Subscription Azure for Students
Resource Group az104-rg7
Name vnet1
Region East US

Security

Azure Bastion Disabled
Azure Firewall Disabled
Azure DDoS Network Protection Disabled

IP addresses

[Previous](#)

[Next](#)

[Create](#)

[Give feedback](#)

- Wait for the virtual network to deploy, and then select Go to resource.

Microsoft Azure Search resources, services, and docs (G+)

Home > vnet1-1720093293545 | Overview >

vnet1 Virtual network

Search

Move Delete Refresh Give feedback

Overview

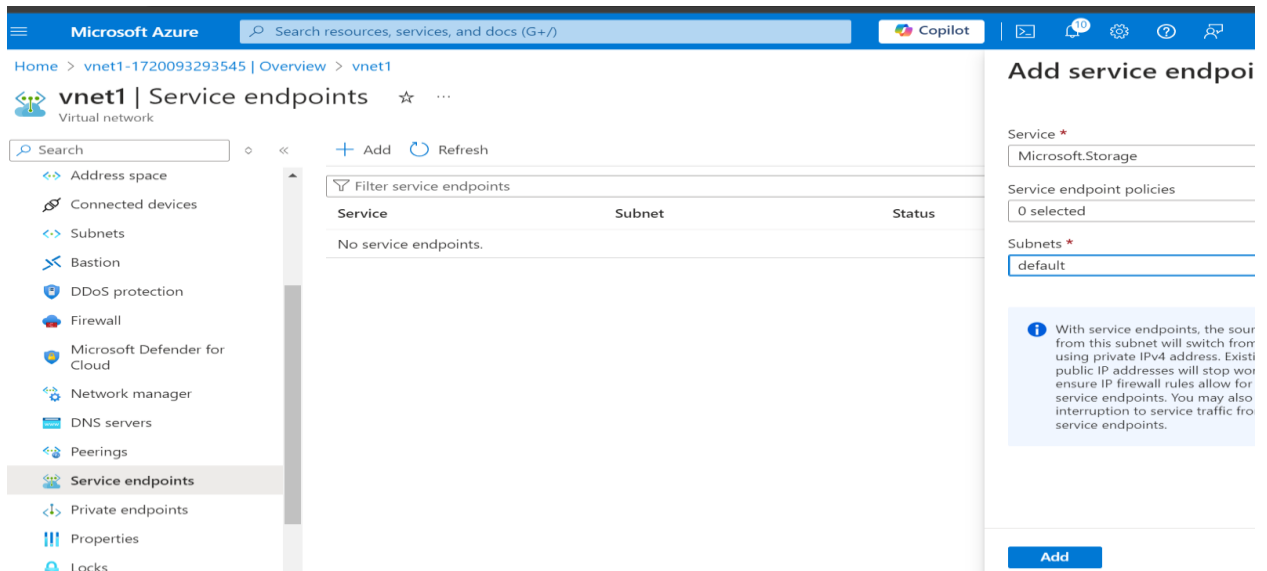
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
 - Address space
 - Connected devices
 - Subnets
 - Bastion
 - DDoS protection
 - Firewall
 - Microsoft Defender for Cloud

Essentials

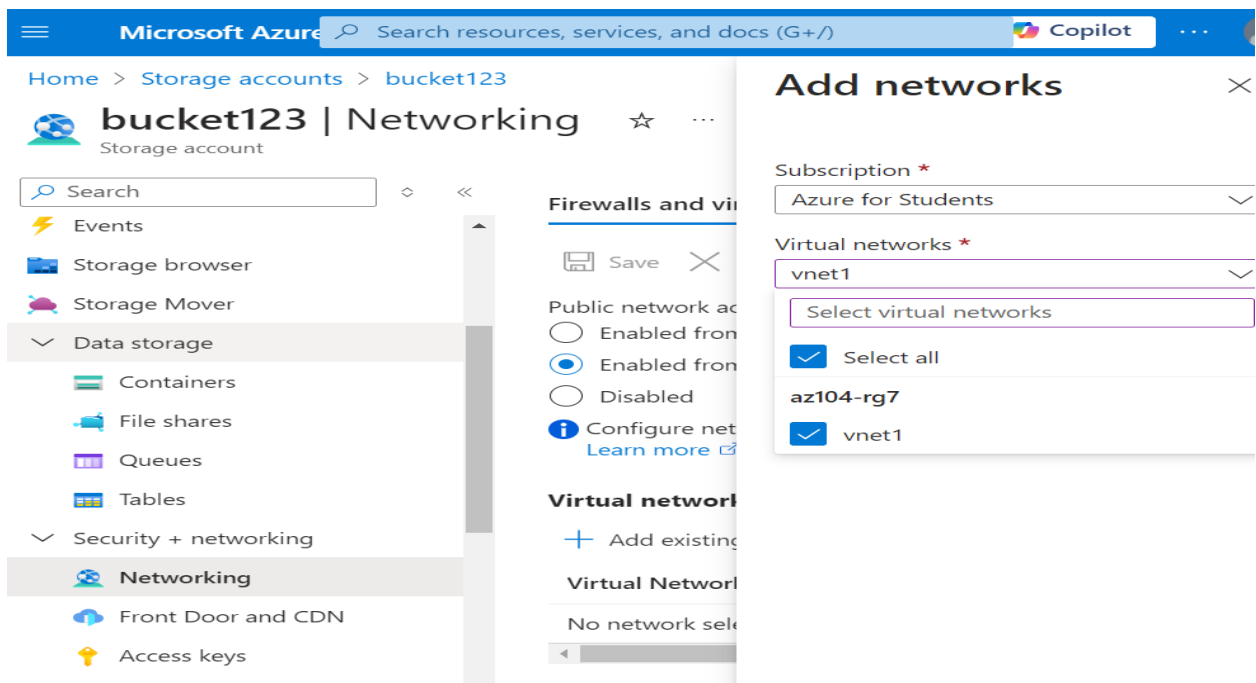
Resource group (move) az104-rg7	Address space 10.0.0.0/16
Location (move) East US	DNS servers Azure provided DNS service
Subscription (move) Azure for Students	Flow timeout Configure
Subscription ID 4f3c0128-9784-4d96-90c6-34c866282c32	BGP community string Configure
Tags (edit) Add tags	Virtual network ID 70a4da6f-b8f9-4b8b-882d-aef8e9d47034

Topology Properties Capabilities (5) Recommendations Tutorials

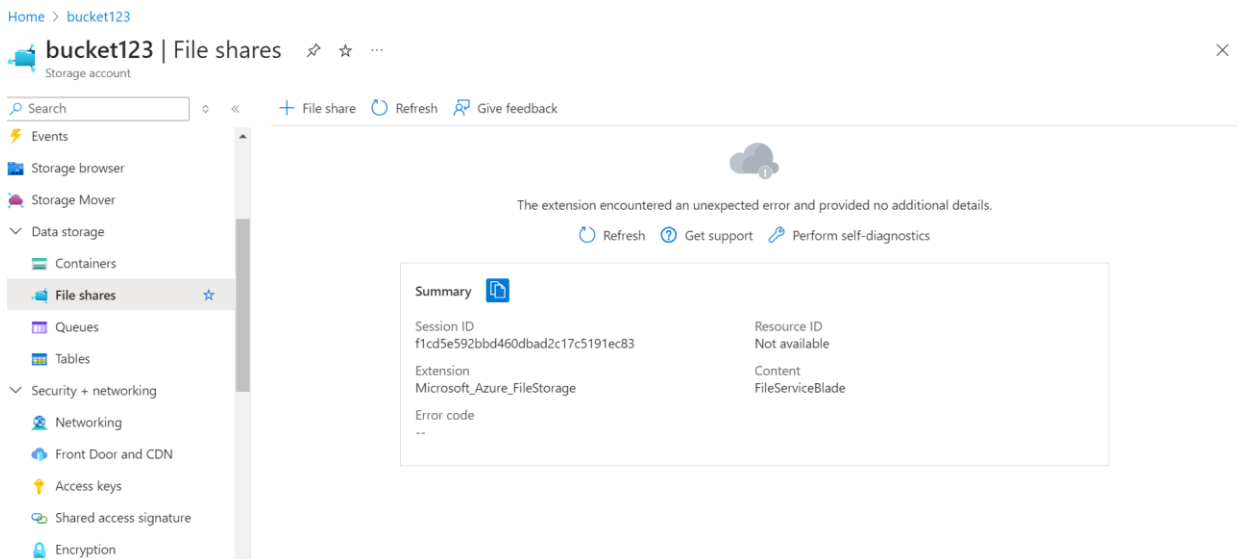
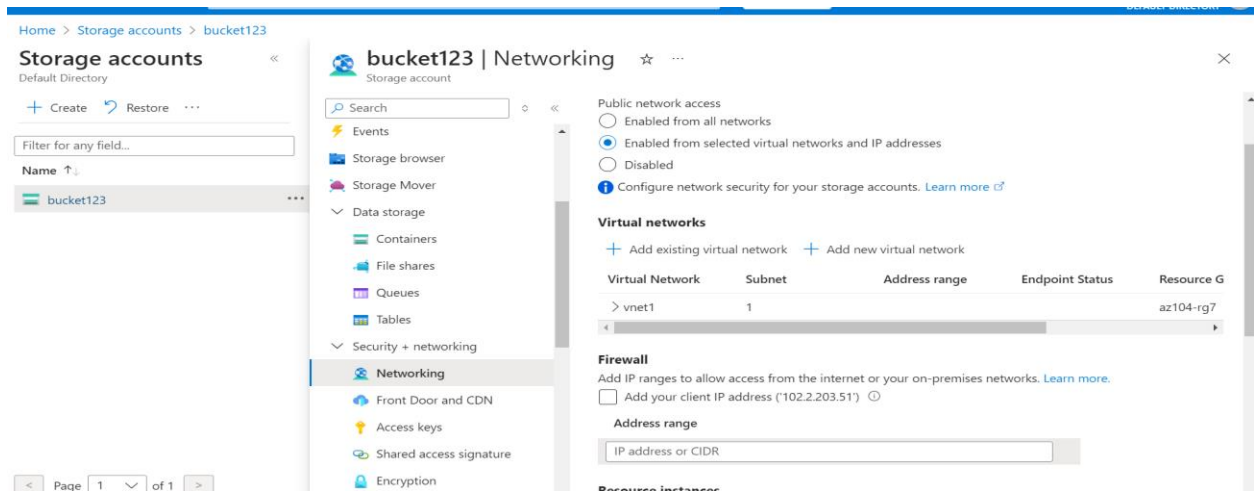
- In the Settings section, select the Service endpoints blade.
- ✓ Select Add.
- ✓ In the Services drop-down select Microsoft.Storage.
- ✓ In the Subnets drop-down check the Default subnet.
- ✓ Click Add to save your changes.
- ✓ Return to your storage account.



- In the Security + networking section, select the Networking blade.
- Select add existing virtual network and select vnet1 and default subnet, select Add.



- In the Firewall section, Delete your machine IP address. Allowed traffic should only come from the virtual network.
- Be sure to Save your changes.



Conclusion

This lab exercise provided a deep dive into the foundational elements of Azure storage services, highlighting the critical aspects of creating and securing various types of storage. Task one involved creating and configuring a storage account, which is the cornerstone of Azure storage services. This task reinforced the importance of proper setup and configuration to ensure scalability, cost-efficiency, and robust performance of our storage solutions. It also underscored the versatility of Azure storage accounts in supporting diverse storage needs, from general-purpose use cases to specialized scenarios requiring advanced data handling capabilities.

Task two focused on creating and securing blob storage, which is essential for storing large amounts of unstructured data like logs, media files, and backups. This task highlighted the significance of implementing security best practices, such as setting up role-based access control (RBAC) and encryption, to protect sensitive data from unauthorized access and potential breaches. We also explored how to efficiently manage and optimize blob storage to support data-intensive applications.

Finally task three addressed the creation and configuration of secure Azure file storage. This task emphasized the importance of providing secure, scalable, and accessible file shares for applications and services. It reinforced the need to implement secure access methods, such as network file sharing over SMB (Server Message Block) with encryption and integration with Azure Active Directory, to ensure data integrity and availability. Together, these tasks highlighted the critical role of secure and well-managed storage solutions in supporting the seamless operation and security of cloud-based applications in the real world scenerios.