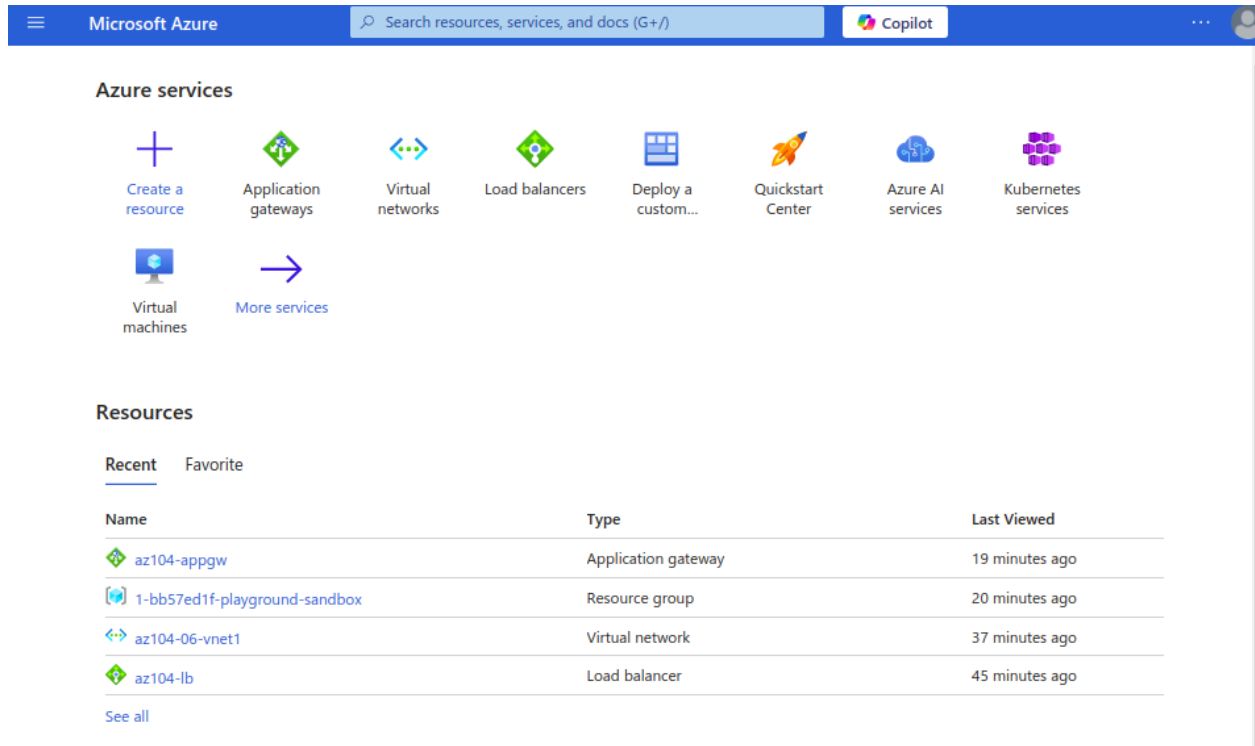


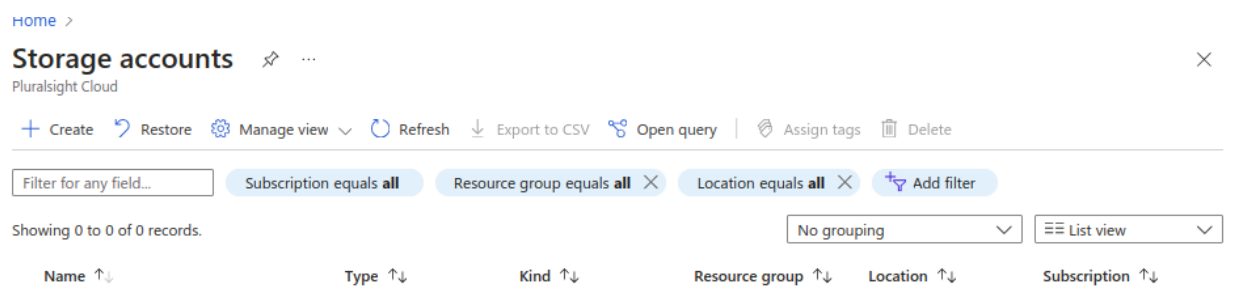
Lab 07 - Manage Azure Storage

Task 1: Create and configure a storage account.

1. Sign in to the Azure portal - <https://portal.azure.com>.



2. Search for and select Storage accounts, and then click + Create.



3. On the Basics tab of the Create a storage account blade, specify the following settings (leave others with their default values):

Create a storage account ...

Basics

Advanced

Networking

Data protection

Encryption



Tags

Review + create

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#) 









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 *	P8-Real Hands-On Labs 
Resource group *	1-bb57ed1f-playground-sandbox 

[Create new](#)

Instance details

Storage account name * 	az104katerynabakhmat
Region * 	(US) East US 
	Deploy to an Azure Extended Zone
Primary service 	Select a primary service 
Performance * 	<input checked="" type="radio"/> Standard: Recommended for most scenarios (general-purpose v2 account) <input type="radio"/> Premium: Recommended for scenarios that require low latency.
Redundancy * 	Geo-redundant storage (GRS) 
	<input checked="" type="checkbox"/> Make read access to data available in the event of regional unavailability.

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

Home / Storage accounts /

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

Permitted scope for copy operations (preview)

Hierarchical Namespace

Hierarchical namespace, complemented by Data Lake Storage Gen2 endpoint, enables file and directory semantics, accelerates big data analytics workloads, and enables access control lists (ACLs) [Learn more](#)

Enable hierarchical namespace ☐

Access protocols

Blob and Data Lake Gen2 endpoints are provisioned by default [Learn more](#)

Enable SFTP ☐
i SFTP can only be enabled for hierarchical namespace accounts

Enable network file system v3 ☐
i To enable NFS v3 'hierarchical namespace' must be enabled. [Learn more about NFS v3](#)

Blob storage

Allow cross-tenant replication ☐

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

[Give feedback](#)

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

Home / Storage accounts /

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

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

Home / Storage accounts /

Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review + 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 ⓘ

☒ 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 ⓘ

☒ Enable soft delete for file shares
Soft delete enables you to recover file shares that were previously marked for deletion. [Learn more](#)

Days to retain deleted file shares ⓘ

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

Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review + 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 ⓘ

☐

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

Create a storage account ...

Basics Advanced Networking Data protection Encryption Tags Review + create

[View automation template](#)

Basics

Subscription	P8-Real Hands-On Labs
Resource group	1-bb57ed1f-playground-sandbox
Location	East US
Storage account name	az104katerynabakhmat
Primary service	
Performance	Standard
Replication	Read-access geo-redundant storage (RA-GRS)

Advanced

Enable hierarchical namespace	Disabled
Enable SFTP	Disabled
Enable network file system v3	Disabled
Allow cross-tenant replication	Disabled
Access tier	Hot
Enable large file shares	Enabled

Security

Secure transfer	Enabled
Blob anonymous access	Disabled
Allow storage account key access	Enabled
Default to Microsoft Entra authorization in the Azure portal	Disabled
Minimum TLS version	Version 1.2
Permitted scope for copy operations (preview)	From any storage account

Networking

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

6. Once the storage account is deployed, select Go to resource.

hmat_1729768285215 | Overview

[Delete](#)
[Cancel](#)
[Redeploy](#)
[Download](#)
[Refresh](#)

Your deployment is complete

Deployment name: az104kater... Start time: 10/24/2024, 2:11:48 ...
 Subscription: P8-Real Hands-On... Correlation ID: baaf5afb-c34b-40b...
 Resource group: 1-bb57ed1f-p...

Deployment details
 Next steps

[Go to resource](#)

7. 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.

Home > az104katernabakhmat_1729768285215 | Overview >

az104katernabakhmat

Storage account

[Upload](#)
[Open in Explorer](#)
[Delete](#)
[Move](#)
[Refresh](#)
[Open in mobile](#)
[CLI / PS](#)

[Overview](#)

[Activity log](#)
[Tags](#)
[Diagnose and solve problems](#)
[Access Control \(IAM\)](#)
[Data migration](#)
[Events](#)
[Storage browser](#)
[Storage Mover](#)
[Partner solutions](#)
 > Data storage
 > Security + networking
 > Data management
 > Settings
 > Monitoring
 > Monitoring (classic)
 > Automation
 > Help

Essentials

[JSON View](#)

Resource group ([move](#))
[1-bb57ed1f-playground-sandbox](#)

Location
 eastus

Primary/Secondary Location
 Primary: East US, Secondary: West US

Subscription ([move](#))
[P8-Real Hands-On Labs](#)

Subscription ID
 9734ed68-621d-47ed-babd-269110dbac1

Disk state
 Primary: Available, Secondary: Available

Tags ([edit](#))
[Add tags](#)

Performance
 Standard

Replication
 Read-access geo-redundant storage (RA-GRS)

Account kind
 StorageV2 (general purpose v2)

Provisioning state
 Succeeded

Created
 10/24/2024, 2:11:50 PM

[Properties](#)
[Monitoring](#)
[Capabilities \(7\)](#)
[Recommendations \(0\)](#)
[Tutorials](#)
[Tools + SDKs](#)

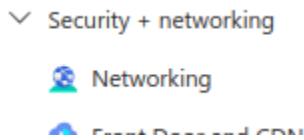
Blob service

Hierarchical namespace [Disabled](#)
 Default access tier [Hot](#)
 Blob anonymous access [Disabled](#)
 Blob soft delete [Enabled \(7 days\)](#)
 Container soft delete

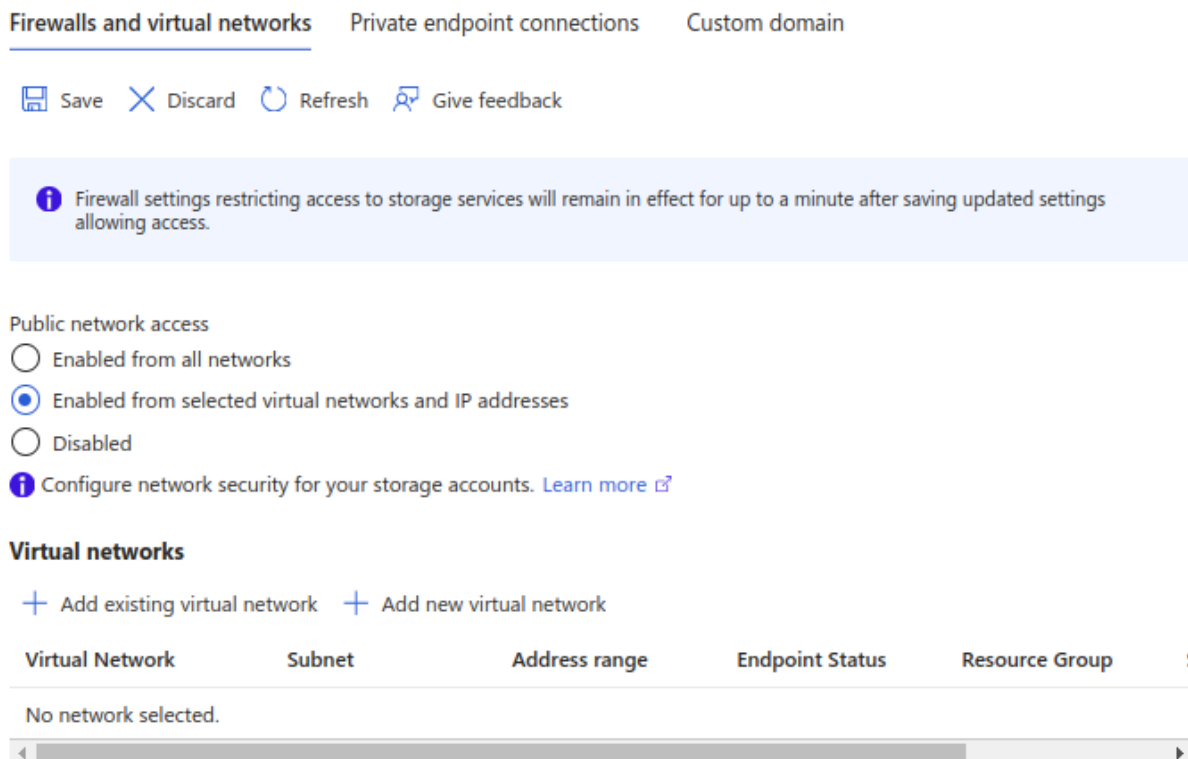
Security

Require secure transfer for REST API operations [Enabled](#)
 Storage account key access [Enabled](#)
 Minimum TLS version [Version 1.2](#)
 Infrastructure encryption [Disabled](#)

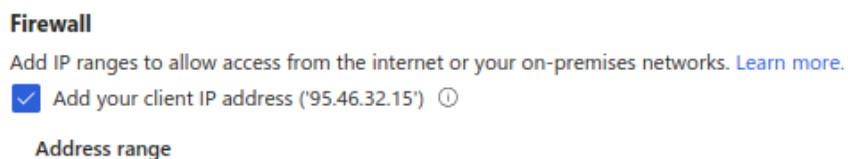
8. In the Security + networking section, select Networking. Notice public network access is disabled.



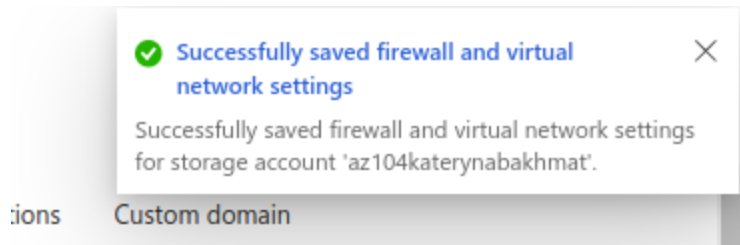
Change the public access level to Enabled from selected virtual networks and IP addresses.



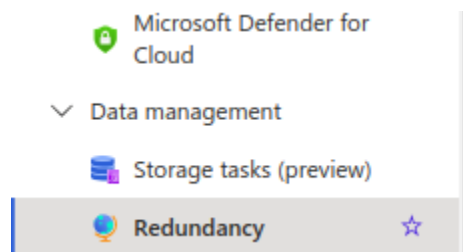
In the Firewall section, check the box for Add your client IP address.



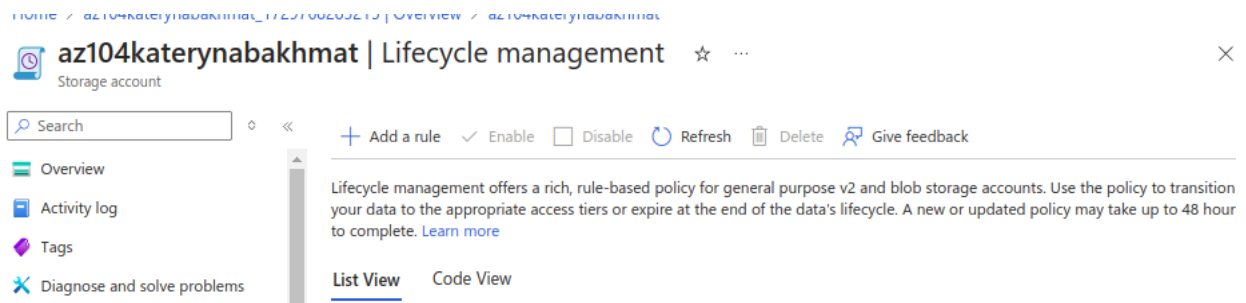
Be sure to Save your changes.



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



10. 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.

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

☐ Snapshots

☐ Versions

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.

Add a rule

1 Details 2 Base blobs

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

Delete the blob

↓

+ Add conditions

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

[Previous](#) [Add](#)

Task 2: Create and configure secure blob storage

Create a blob container and a time-based retention policy

1.Continue in the Azure portal, working with your storage account.

2.In the Data storage section, click Containers.

The screenshot shows the Azure portal interface for a storage account named 'az104katerynabakhmat'. The left sidebar shows the navigation menu with 'Data storage' expanded and 'Containers' selected. The main content area displays the 'Containers' page with a search bar, a list of containers, and a table of container details.

Name	Last modified	Anonymous access l...	Lease state
\$logs	10/24/2024, 2:12:14 ...	Private	Available

3.Click + Container and Create a container with the following settings:

New container

Name *

data

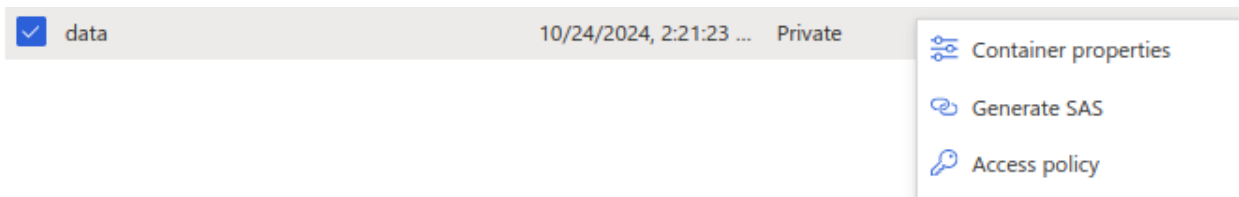
Anonymous access level ⓘ

Private (no anonymous access)

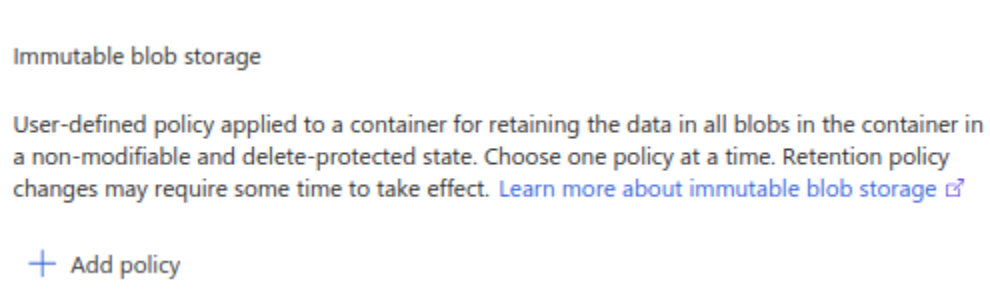
The access level is set to private because anonymous access is disabled on this storage account.

Advanced

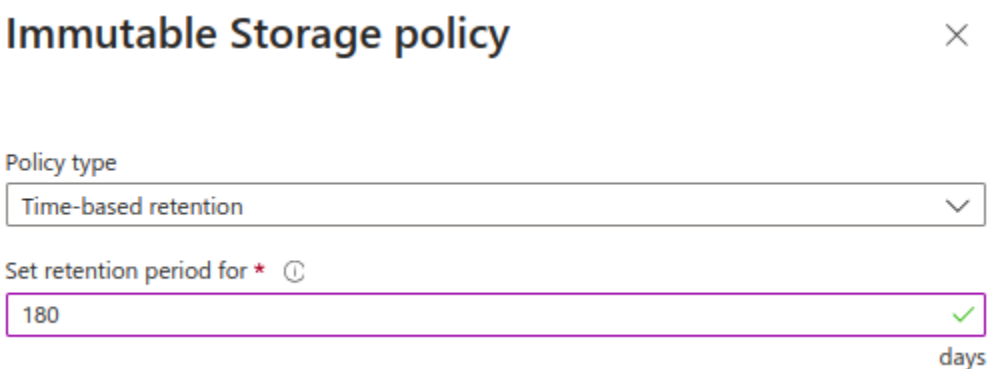
4. On your container, scroll to the ellipsis (...) on the far right, select Access Policy.



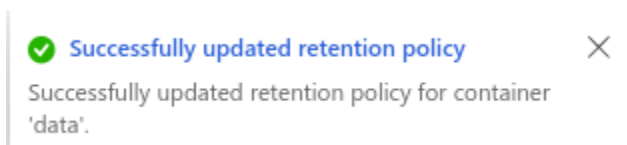
5. In the Immutable blob storage area, select Add policy.



6. In the Immutable blob storage area, select Add policy.



6. Select Save.



Manage blob uploads

1. Return to the containers page, select your data container and then click Upload.

data

Container

Search

◊

«

Overview

Diagnose and solve problems

Access Control (IAM)

Settings

Upload

Change access level

Refresh

Delete

Change tier

Acquire lease

Break lease

View snapshots

⋮

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

Location: data

Search blobs by prefix (case-sensitive)


Show deleted blobs

Add filter

Name	Modified	Access tier	Archive status	Blob type
No results				

2. On the Upload blob blade, expand the Advanced section.

Upload files



1 file(s) selected: images.jpeg

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

☐ Overwrite if files already exist

^ Advanced

Blob type ⓘ

Block blob

☒ Upload .vhd files as page blobs (recommended)

Block size ⓘ

4 MiB

Access tier ⓘ

Hot (Inferred)

Upload to folder

securitytest

Blob index tags ⓘ

Key

Value

Encryption scope

☒ Use existing default container scope

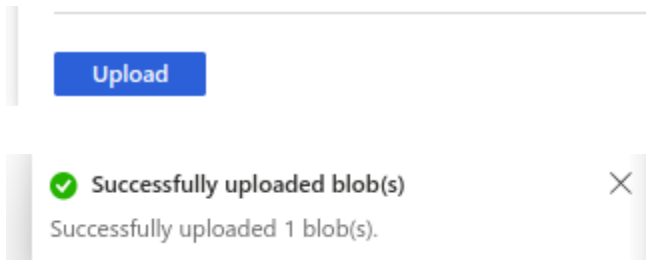
☐ Choose an existing scope

Retention policy ⓘ

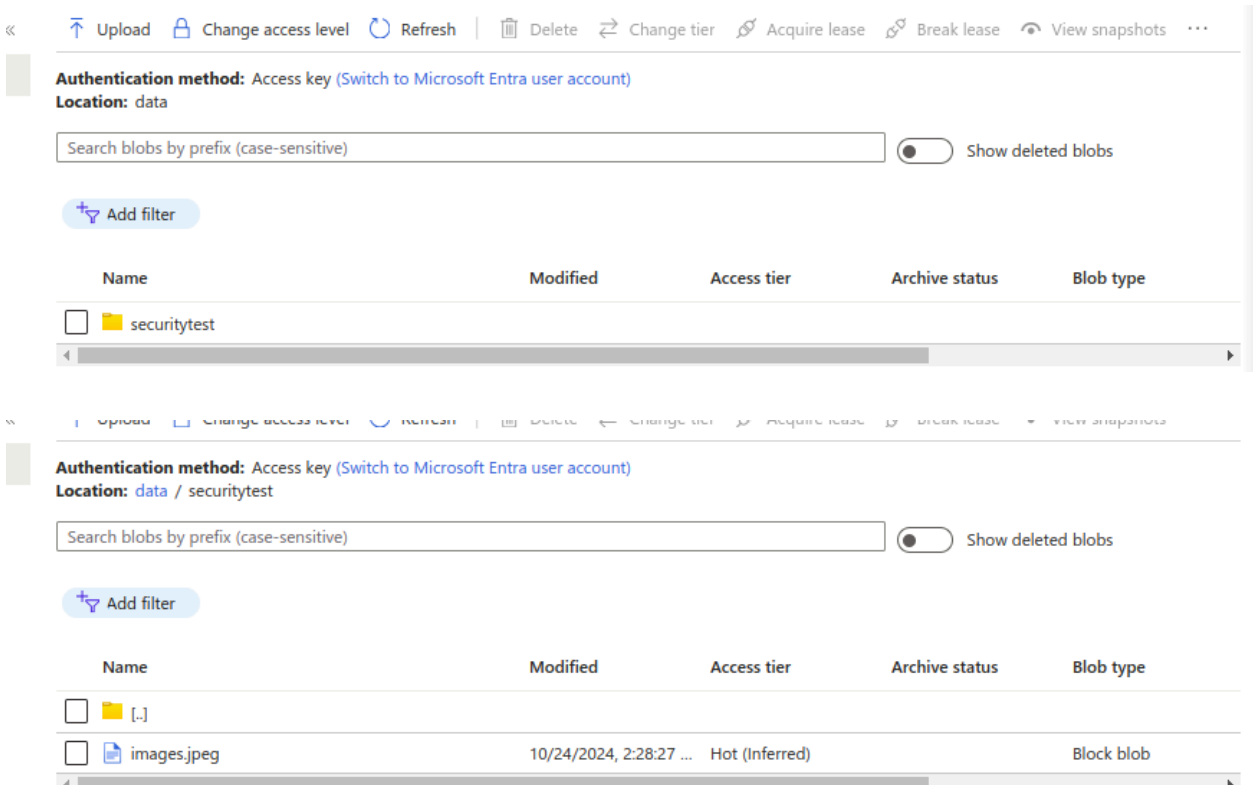
☒ Use container-level retention period: 180 day(s)

☐ Choose custom retention period

3. Click Upload.



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



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

« Upload Change access level Refresh Delete Change tier Acquire lease Break lease View snapshots ...

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

Search blobs by prefix (case-sensitive) ☐ Show deleted blobs

+ Add filter

Name	Modified	Access tier	Archive status	Blob type
[-]				
images.jpeg	10/24/2024, 2:28:27 ...	Hot (Inferred)		Block blob

6. Copy the file URL and paste into a new Inprivate browsing window.

securitytest/images.jpeg ...

Blob

Save Discard Download Refresh Delete Change tie

Overview Versions Snapshots Edit Generate SAS

Properties

URL

7. You should be presented with an XML-formatted message stating ResourceNotFound or PublicAccessNotPermitted.

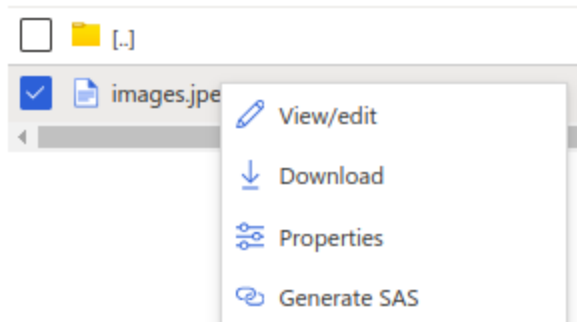
az104katerynabakhmat.blob.core.win... | University Softserve ask alsa - How to s... DevOps needs cloudguru

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

```
<?xml version="1.0" encoding="utf-8" ?>
<Error>
  <Code>PublicAccessNotPermitted</Code>
  <Message>Public access is not permitted on this storage account. RequestId:486c330a-101e-0017-0f08-2692f4000000 Time:2024-10-24T11:31:01.1470315Z</Message>
</Error>
```

Configure limited access to the blob storage

1. 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):



Overview Versions Snapshots Edit Generate SAS

A shared access signature (SAS) is a URI that grants restricted access to an Azure Storage blob. Use it when you want to grant your storage account key. [Learn more about creating an account SAS](#)

Signing method

☒ Account key ☐ User delegation key

Signing key ⓘ

Key 1 ▼

Stored access policy

None ▼

Permissions * ⓘ

Read ▼

Start and expiry date/time ⓘ

Start

10/23/2024 2:32:06 PM

(UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius ▼

Expiry

11/01/2024 10:32:06 PM

(UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius ▼

Allowed IP addresses ⓘ

for example, 168.1.5.65 or 168.1.5.65-168.1....

Allowed protocols ⓘ

☒ HTTPS only ☐ HTTPS and HTTP

Generate SAS token and URL

2.Click Generate SAS token and URL.

Generate SAS token and URL

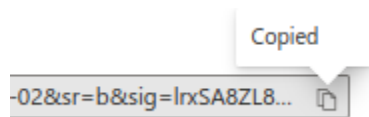
Blob SAS token ⓘ

sp=r&st=2024-10-23T11:32:06Z&se=2024-11-01T20:32:06Z&spr=https&sv=2022-11-02&sr=b&sig=lrSA8ZL8kTAHgB734IZUmhBUph5fDWhwvYpmfWQkwY%3D

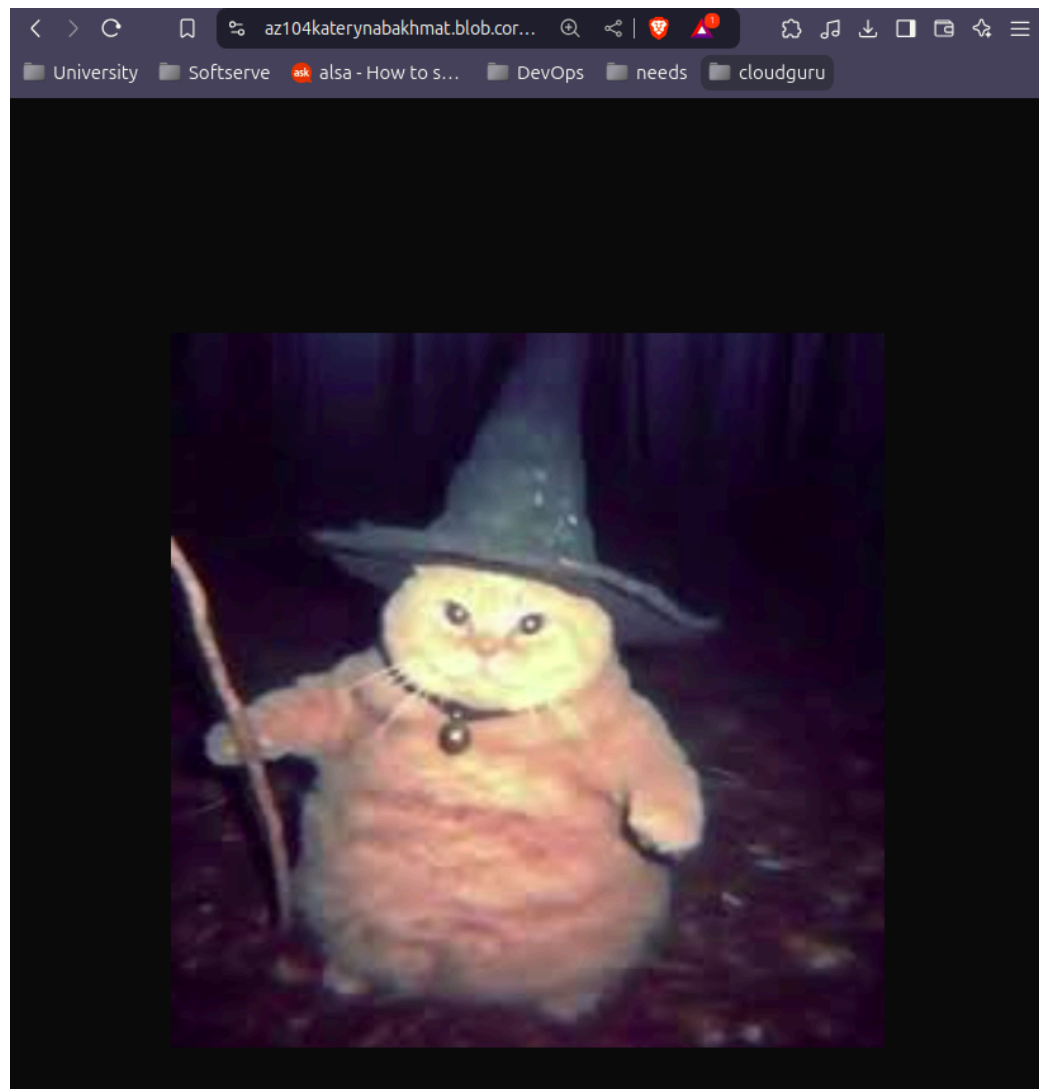
Blob SAS URL

https://az104katerynabakhmat.blob.core.windows.net/data/securitytest/images.jpeg?sp=r&st=2024-10-23T11:32:06Z&se=2024-11-01T20:32:06Z&spr=https&sv=2022-11-02&sr=b&sig=lrSA8ZL8...

3. Copy the Blob SAS URL entry to the clipboard.



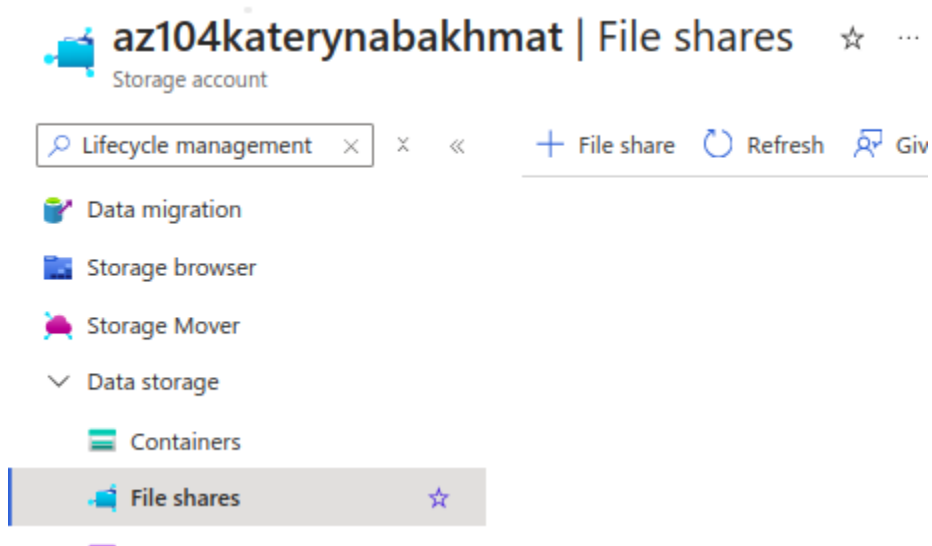
4. Open another InPrivate browser window and navigate to the Blob SAS URL you copied in the previous step.



Task 3: Create and configure an Azure File storage

Create the file share and upload a file

1. In the Azure portal, navigate back to your storage account, in the Data storage section, click File shares.



2. Click + File share and on the Basics tab give the file share a name, share1.

New file share ...

Basics Backup Review + create

Name *	<input type="text" value="share1"/>
Access tier *	<input type="text" value="Transaction optimized"/>

Performance

Maximum IO/s ⓘ	20000
Maximum capacity	100 TiB

3. Notice the Access tier options. Keep the default Transaction optimized.

Access tier *

Transaction optimized




4. Move to the Backup tab and ensure Enable backup is not checked. We are disabling backup to simplify the lab configuration.

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

☐

5. Click Review + create, and then Create. Wait for the file share to deploy.

✓ Validation passed

Basics

Backup

Review + create

Basics

File share name

share1

Access Tier

TransactionOptimized

Protocol

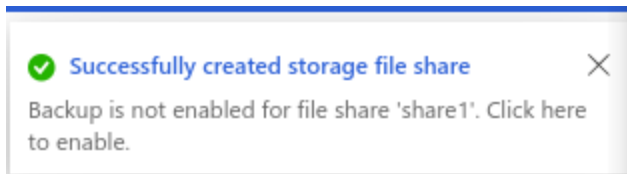
SMB

Create

< Previous

Next >

[Download a template for automation](#)

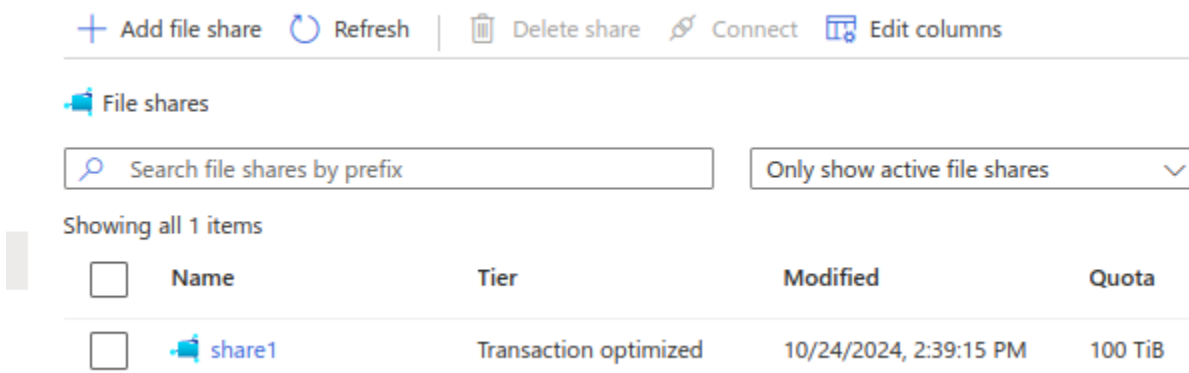
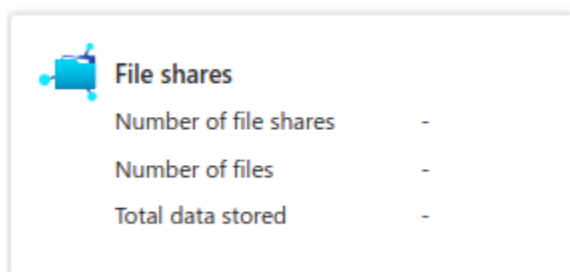


Explore Storage Browser and upload a file

1.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.



2.Select File shares and verify your share1 directory is present.



3. Select your share1 directory and notice you can + Add directory. This lets you create a folder structure.

The screenshot shows the OneDrive web interface for a directory named 'share1'. At the top, there is a toolbar with buttons for 'Upload', 'Add directory', 'Refresh', 'Delete', 'Copy', 'Paste', and a menu icon. Below the toolbar, the breadcrumb 'File shares > share1' is visible. The 'Authentication method' is set to 'Access key' with a link to 'Switch to Microsoft Entra user account'. A search bar is present with the placeholder text 'Search files by prefix'. Below the search bar, it says 'Showing all 0 items'. A table with columns 'Name', 'Type', and 'Size' is shown, but it is empty with the message 'No items found'. A 'New directory' dialog box is open in the foreground. The dialog has a title 'New directory' and a label 'Name'. The input field contains the text 'directory'. There are 'Ok' and 'Cancel' buttons at the bottom right of the dialog. The background interface is partially obscured by the dialog box.

Upload Add directory Refresh Delete Copy Paste ...

File shares > share1

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

Search files by prefix

Showing all 0 items

	Name	Type	Size
	No items found		

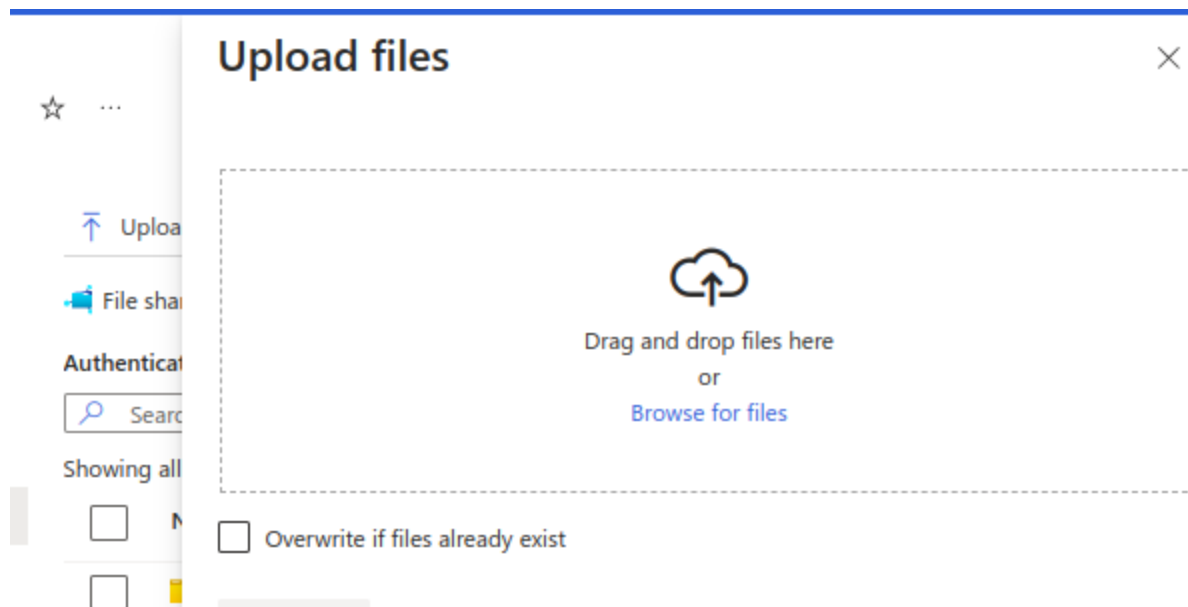
New directory

Name

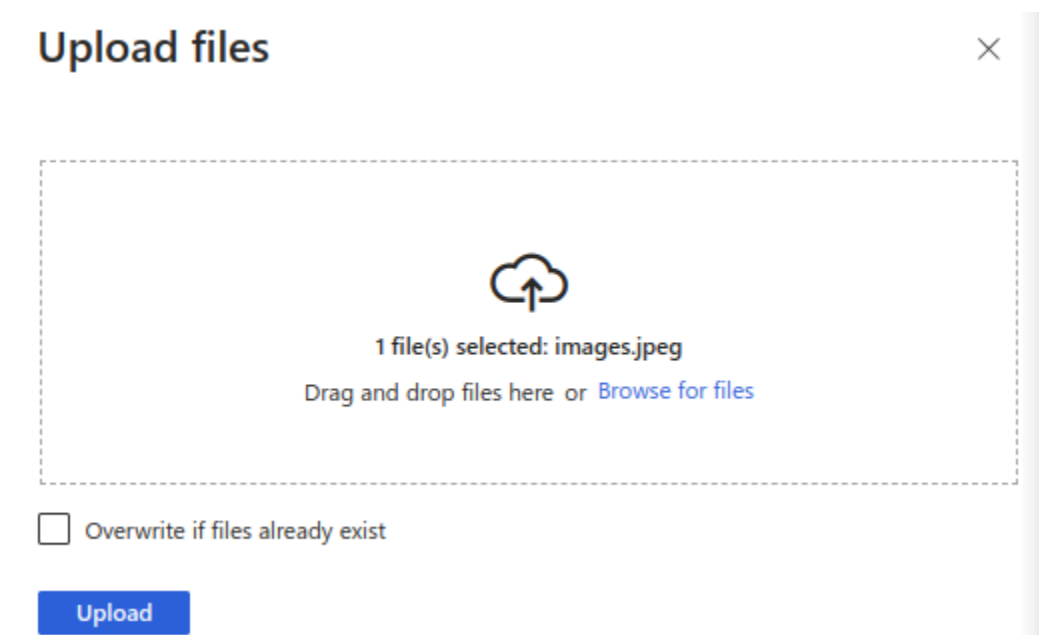
Ok Cancel

	Name	Type	Size
	No items found		

4. Select Upload. Browse to a file of your choice, and then click Upload.



images.jpeg	4.9 kB	Image	14:27
-------------	--------	-------	-------



Current uploads

Dismiss: [Completed](#) [All](#)

images.jpeg

✓ 4.78 KiB / 4.78 KiB

Restrict network access to the storage account

1. In the portal, search for and select Virtual networks.

The screenshot shows the Azure portal interface. At the top, a search bar contains the text 'virtual network'. Below the search bar, there are tabs for 'All', 'Services (51)', 'Marketplace (7)', and 'More (4)'. The 'Services' section is expanded, showing 'Virtual networks' with a 'See more' link. Below this, the 'Virtual networks' page is displayed. It includes a 'Home >' breadcrumb, a title 'Virtual networks', and a 'Pluralsight Cloud' label. There are several action buttons: '+ Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. A filter bar shows 'Subscription equals all', 'Resource group equals all', and 'Location equals all'. The table below shows one record for a virtual network named 'az104-06-vnet1' in the '1-bb57ed1f-playground-sandbox' resource group, located in 'East US' under the 'P8-Real Hands-On Labs' subscription.

Name ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓
az104-06-vnet1	1-bb57ed1f-playground-sandbox	East US	P8-Real Hands-On Labs

2. Select + Create. Select your resource group. and give the virtual network a name, vnet1.

Create virtual network ...

- Basics
- Security
- IP addresses
- Tags
- Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

[Learn more.](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

P8-Real Hands-On Labs

Resource group *

1-bb57ed1f-playground-sandbox

Create new

Instance details

Virtual network name *

vnet1

Region * ⓘ

(US) East US

Deploy to an Azure Extended Zone

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

Create virtual network ...

Basics Security IP addresses Tags Review + create

[View automation template](#)

Basics

Subscription	P8-Real Hands-On Labs
Resource Group	1-bb57ed1f-playground-sandbox
Name	vnet1
Region	East US

Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

IP addresses

Address space	10.0.0.0/16 (65,536 addresses)
Subnet	default (10.0.0.0/24) (256 addresses)

Tags

3. Take the defaults for other parameters, select Review + create, and then Create.

0529121 | Overview

Deployment is in progress

Deployment name : vnet1-1729770529121 Start time : 10/24/2024, 2:48:55 PM
Subscription : P8-Real Hands-On Labs Correlation ID : 9b25441e-a7ef-4d21-9541...
Resource group : 1-bb57ed1f-playground-s...

Deployment details

Resource	Type	Status
vnet1	Virtual network	Created

Deployment succeeded

Deployment 'vnet1-1729770529121' to resource group '1-bb57ed1f-playground-sandbox' was successful.

Go to resource Pin to dashboard

Microsoft Defender for Cloud

Secure your apps and infrastructure

Go to Microsoft Defender for Cloud >

Free Microsoft tutorials

Start learning today >

Work with an expert

Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.

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

Your deployment is complete

Deployment name : vnet1-1729770529121 Start time : 10/24/2024, 2:48:55 PM
Subscription : P8-Real Hands-On Labs Correlation ID : 9b25441e-a7ef-4d21-9541...
Resource group : 1-bb57ed1f-playground-s...

Deployment details

Next steps

Go to resource

5.In the Settings section, select the Service endpoints blade.

Select Add.

Settings

Address space

Connected devices

Subnets

Bastion

DDoS protection

Firewall

Microsoft Defender for Cloud

Network manager

DNS servers

Peerings

Service endpoints

S

P

S

9

Ti

A

Ti

+ Add

Refresh

Filter service endpoints

Service	Subnet	Status	Locations
No service endpoints.			

In the Services drop-down select Microsoft.Storage.

Add service endpoints

Service *

Microsoft.Storage

In the Subnets drop-down check the Default subnet.

Subnets *

default

Click Add to save your changes.

Add

6. Return to your storage account.

az104katerynabakhmat Storage account

Search

Overview

- Activity log
- Tags
- Diagnose and solve problems

Essentials

Resource group (move)
[1-bb57ed1f-playground-sandbox](#)

Location
eastus

Performance
Standard

Replication
Read-access geo-redundant storage (RA-GRS)

JSON View

7. In the Security + networking section, select the Networking blade.

az104katerynabakhmat | Networking

Search

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Storage Mover

Partner solutions

Data storage

- Containers
- File shares
- Queues
- Tables

Security + networking

Networking

Firewalls and virtual networks Private endpoint connections Custom domain

Save Discard Refresh Give feedback

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	Subscription
No network selected.					

Firewall



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

Address range

8. Select add existing virtual network and select vnet1 and default subnet, select Add.

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	Subscription
-----------------	--------	---------------	-----------------	----------------	--------------

Add networks



Subscription *


Virtual networks *

Subnets *

9. In the Firewall section, Delete your machine IP address. Allowed traffic should only come from the virtual network.

Firewall

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

☐ Add your client IP address ('95.46.32.15') 

Address range

10. Be sure to Save your changes.

<< **Firewalls and virtual networks** Private endpoint connections Custo

Save Discard Refresh Give feedback

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

✓ **Successfully saved firewall and virtual network settings** ✕

Successfully saved firewall and virtual network settings for storage account 'az104katerynabakhmat'.

11. Select the Storage browser and Refresh the page. Navigate to your file share or blob content.

Sto ✕ ✕ <<

Storage browser

az104katerynabakhmat <

Favorites

> Recently viewed

Blob containers

▼ File shares

share1

[View all](#)

Queues

Tables

This request is not authorized to perform this operation.

Summary

Session ID	Resource ID
2384a3ec5b764909af22b48ece1f6ac9	/subscriptions/9734ed68-621d-47ed-babd-2691...
Extension	Content
Microsoft_Azure_Storage	FilesBlade
Error code	Storage Request ID
403	25b1d43a-c01a-00fb-270c-269a8d000000

Details

- This request is not authorized to perform this operation. RequestId:25b1d43a-c01a-00fb-270c-269a8d000000 Time:2024-10-24T12:02:55.5193096Z
- This storage account's 'Firewalls and virtual networks' settings may be blocking access to storage services. Try adding your client IP address ('95.46.32.15') to the firewall exceptions, or by allowing access from 'all networks' instead of 'selected networks'. [Learn more](#)