

Manage Azure Storage

| | |
|---|----|
| Manage Azure Storage | 1 |
| Task 1: Create and configure a storage account. | 1 |
| Task 2: Create and configure secure blob storage. | 10 |
| Task 3: Create and configure secure Azure file storage. | 15 |

Task 1: Create and configure a storage account.

Storage accounts:

[Home](#) > [Storage accounts](#) >

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 *

P4-Real Hands-On Labs

Resource group *

1-88b31444-playground-sandbox

Create new

Instance details

Storage account name * ⓘ

vladuslav122

Region * ⓘ

(US) East US

Deploy to an Azure Extended Zone

Primary service ⓘ

Select a primary service

Performance * ⓘ

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

☐ Premium: Recommended for scenarios that require low latency.

Redundancy * ⓘ

Geo-redundant storage (GRS)

☒ Make read access to data available in the event of regional unavailability.

Figure 1. Creating a storage account.

Create a storage account ...

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](#) ↗

Figure 2. Basics.

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

| Name | Subscription | Resource g... | Region | Target sub-... | Subnet | Private DN... |
|------|--------------|---------------|--------|----------------|--------|---------------|
|------|--------------|---------------|--------|----------------|--------|---------------|

Click on add to create a private endpoint

Network routing

Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.

Routing preference * ⓘ

- ☒ Microsoft network routing
- ☐ Internet routing


Figure 3. Networking.

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 ⓘ

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

☒ 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 ⓘ

7

Tracking

Manage versions and keep track of changes made to your blob data.

☐ Enable versioning for blobs
Use versioning to automatically maintain previous versions of your blobs. [Learn more](#) 


Consider your workloads, their impact on the number of versions created, and the resulting costs. Optimize costs by automatically managing the data lifecycle. [Learn more](#) 

Figure 4. Data protection.

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 ⓘ



Figure 5. Encryption.

[Home](#) > [Storage accounts](#) >

Create a storage account ...

Basics Advanced Networking Data protection Encryption Tags **Review + create**

[View automation template](#)

Basics

| | |
|----------------------|--|
| Subscription | P4-Real Hands-On Labs |
| Resource group | 1-88b31444-playground-sandbox |
| Location | East US |
| Storage account name | vladuslav122 |
| 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 |

Previous

Next

Create

Figure 6. Review.

Home > vladuslav122_1742390465099 | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

Your deployment is complete

Deployment name: vladuslav122_1742390465099 Start time: 3/19/2025, 3:21:25 PM
Subscription: P4-Real Hands-On Labs Correlation ID: 9a9390a0-768d-4dd9-8a1d-f98999f3b2b4
Resource group: 1-88b31444-playground-sandbox

Deployment details

Next steps

[Go to resource](#)

Figure 7. Complete deployment.

Home > vladuslav122_1742390465099 | Overview > vladuslav122

Storage account

Search

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Storage Mover

Partner solutions

Resource visualizer

Data storage

Security + networking

Networking

Front Door and CDN

Access keys

Shared access signature

Encryption

Microsoft Defender for Cloud

Data management

Firewalls and virtual networks Private endpoint connections Custom domain

Save Discard Refresh Give feedback

Firewall settings restricting access to storage services will remain in effect for up to a minute after saving updated settings allowing access.

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 Sta |
|----------------------|--------|---------------|--------------|
| 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 ('185.5.253.166')

Address range

IP address or CIDR

Resource instances

Specify resource instances that will have access to your storage account based on their system-assigned managed identity.

| Resource type | Instance name |
|---------------|---------------|
|---------------|---------------|

Figure 8. Networking in a storage account.

Home > vladuslav122_1742390465099 | Overview > vladuslav122

vladuslav122 | Redundancy ☆ ...

Storage account

Search

Save Discard Prepare for failover Refresh Give feedback

Learn more about storage account failover

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Storage Mover

Partner solutions

Resource visualizer

> Data storage

> Security + networking

✓ Data management

Storage tasks (preview)

Redundancy

Data protection

Object replication

Blob inventory

Static website

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 | - |




Figure 9. Redundancy in a storage account.

Add a rule:

Add a rule ...

✓ 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

Move to cool storage

↓

[+ Add conditions](#)

Figure 10. Adding a rule.

[+ 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 the appropriate access tier into effect. [Learn more](#)

[List View](#) [Code View](#)

Enable access tracking ⓘ ☐

| Name | Status | Blob type |
|----------------------------|---------|-----------|
| Movetocool | Enabled | Block |

Figure 11. Created rool.

Task 2: Create and configure secure blob storage.

Create a blob container and a time-based retention policy:

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

Figure 12. Creating a blob container.

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

Figure 13. Configuring storage policy.

Manage blob uploads:

Upload blob



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

Figure 14. Configuring blob.

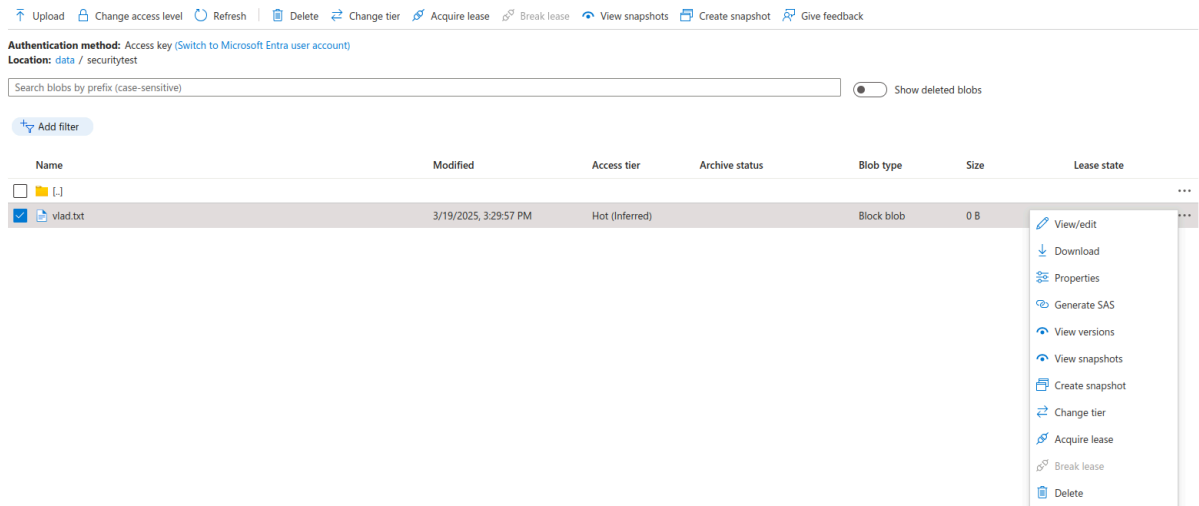
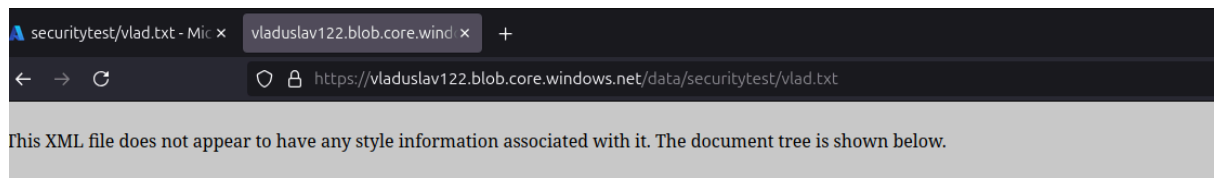


Figure 15. Created blob storage.







```
-<Error>
  <Code>PublicAccessNotPermitted</Code>
-<Message>
  Public access is not permitted on this storage account. RequestId:fc777643-801e-003f-2dd3-98b471000000 Time:2025-03-19T13:31:09.0590251Z
</Message>
</Error>
```

Figure 16. Refused permission.

Configure limited access to the blob storage:

securitytest/vlad.txt ...

Blob

 Save  Discard  Download  Refresh  Delete

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 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

03/18/2025  3:31:43 PM
(UTC+02:00) Athens, Bucharest ▼

Expiry

03/20/2025  11:31:43 PM
(UTC+02:00) Athens, Bucharest ▼

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](#)

Figure 17. Configing SAS.

Since the file is empty, there is nothing here, but it opens:

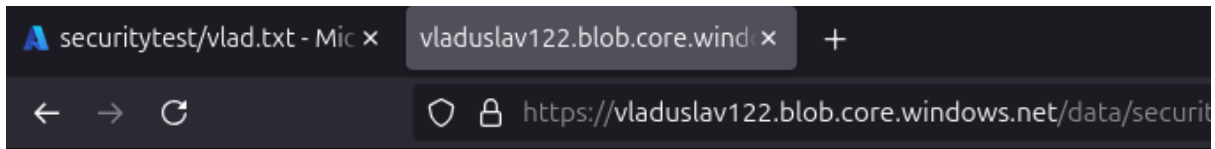


Figure 18. File in blob storage.

Task 3: Create and configure secure Azure file storage.

Create the file share and upload a file:

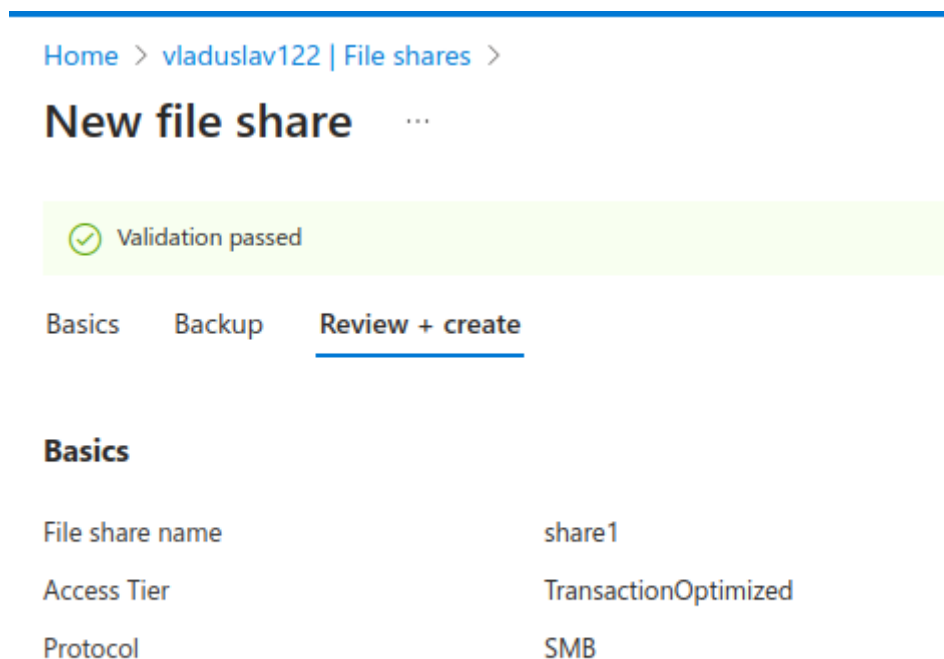


Figure 19. Review file share.

Explore Storage Browser and upload a file:

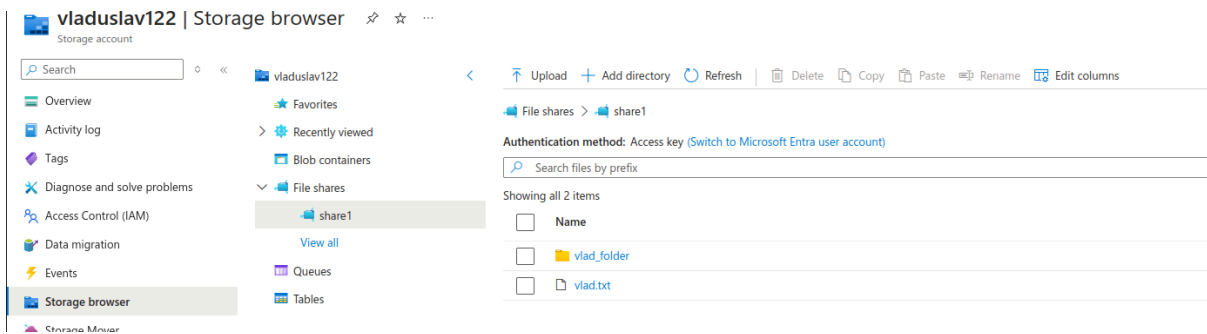


Figure 20. Created file share.

Create virtual network

Basics Security IP addresses Tags Review + create

[View automation template](#)

Basics

| | |
|----------------|-------------------------------|
| Subscription | P4-Real Hands-On Labs |
| Resource Group | 1-88b31444-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

Figure 21. Review virtual network.

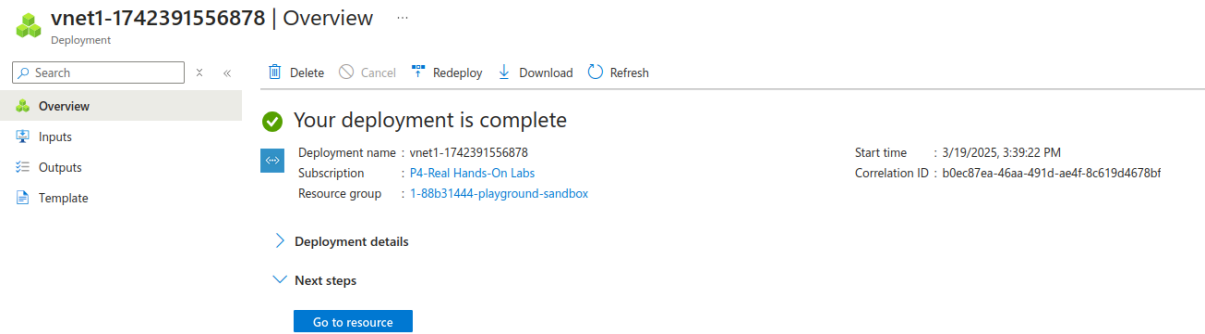


Figure 22. Completed deployment.

Add service endpoints ✕

Service *

Microsoft.Storage ▼

Service endpoint policies

0 selected ▼

Subnets *

default ▼

Figure 23. Adding service endpoints.

Restrict network access to the storage account:

Add networks

Subscription *

P4-Real Hands-On Labs

Virtual networks *

vnet1

Subnets *

default

Select subnets

☒ Select all

vnet1

☒ default

Resource Group

Figure 24. Adding networks.

Figure 26. Checking share1.

vladislav122

Favorites

Recently viewed

Blob containers

\$logs

data

View all

File shares

share1

View all

Queues

Tables

This request is not authorized to perform this operation.

Summary

Session ID
69df2da5a0d547a99c8bf99a723898c8

Resource ID
/subscriptions/0cfe2870-d256-4119-b0a3-16293ac11bd...

Extension
Microsoft_Azure_Storage

Content
BlobsBlade

Error code
403

Storage Request ID
91c7709b-a01e-004a-0ad5-98df5d000000

Details

- This request is not authorized to perform this operation. RequestId:91c7709b-a01e-004a-0ad5-98df5d000000 Time:2025-03-19T13:45:35.2940081Z
- This storage account's 'Firewalls and virtual networks' settings may be blocking access to storage services. Try adding your client IP address ('185.5.253.166') to the firewall exceptions, or by allowing access from 'all networks' instead of 'selected networks'. [Learn more](#)

Figure 27. Checking data.