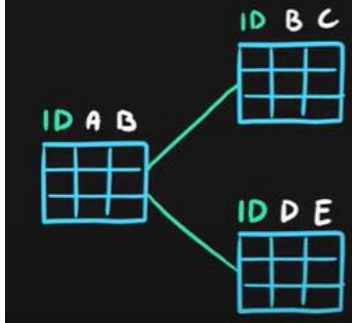


Сховище Azure

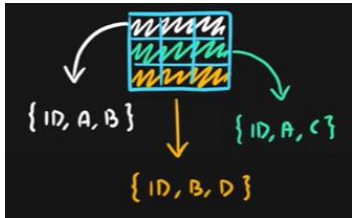
Сховище Azure — це хмарне рішення для зберігання сучасних додатків, що забезпечує високу доступність і масштабованість для задоволення актуальних потреб. Сервіс збереження в Azure має високий ступінь масштабованості, дозволяючи зберігати і обробляти сотні терабайт даних для підтримки сценаріїв з даними великого розміру, які необхідні для дослідницьких, аналітичних фінансових і мультимедійних додатків. На даний момент в Azure зберігаються десятки трильйонів унікальних клієнтських об'єктів і обробляються в середньому мільйони запитів в секунду.

Типи даних

Структуровані дані – можна описати за допомогою схеми



Напівструктуровані дані – дані знаходяться в рядках, але в рядку не можуть бути описані схемою

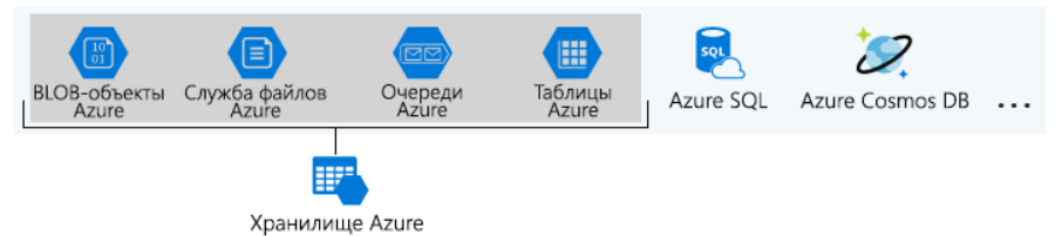


Неструктуровані дані – файли з зображеннями, фільми, текстові файли



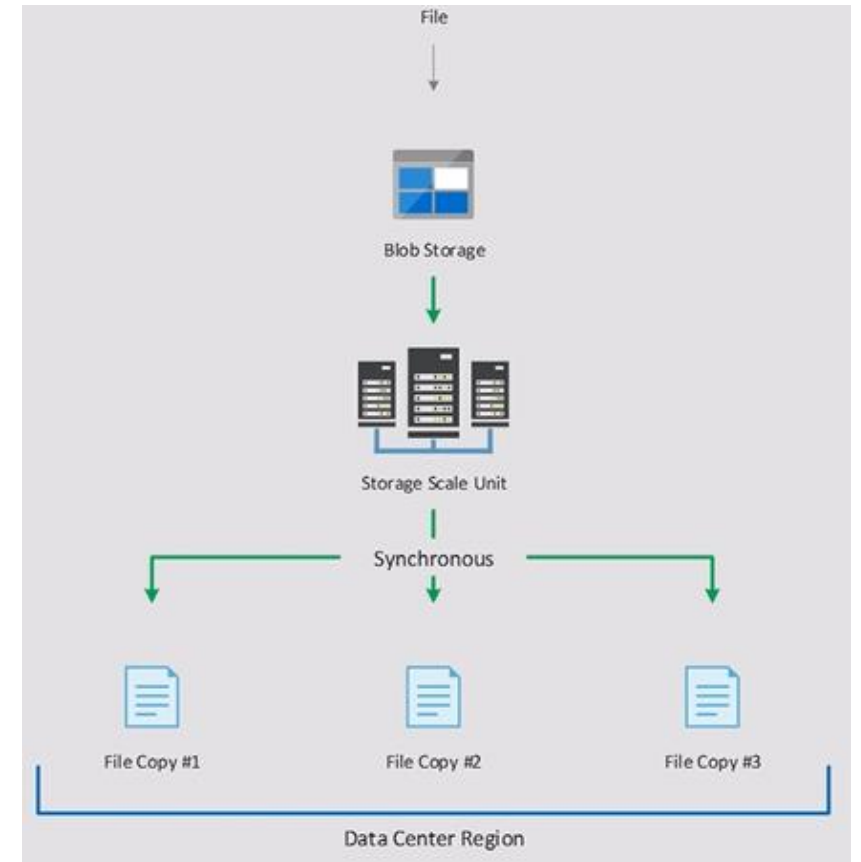
Служби сховища Azure

- Azure об'єднує чотири служби даних під назвою служби сховища Azure.
 - BLOB-об'єкти Azure – сховище для великих текстових та двійкових файлів, тобто неструктурованих даних.
 - Файли Azure – сховище для зберігання файлів.
 - Черги Azure - сховище для зберігання повідомлень.
 - Таблиці Azure – сховище для напівструктурованих даних.

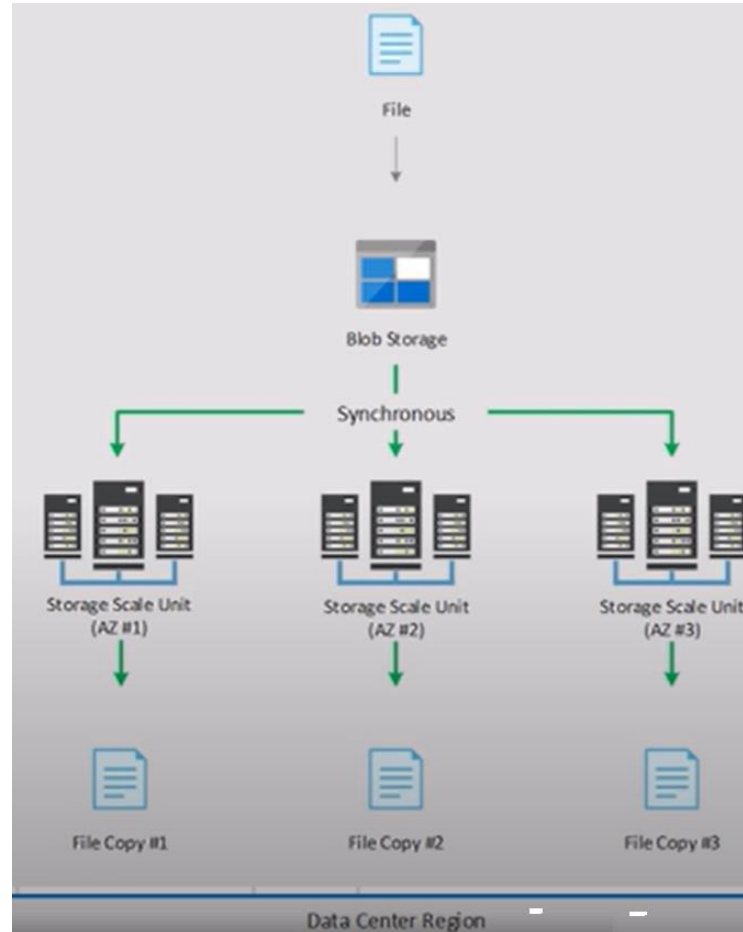


Надлишковість даних (Data Redundance) - Ключова архітектура сховища даних Azure, яка гарантує надійність зберігання даних.

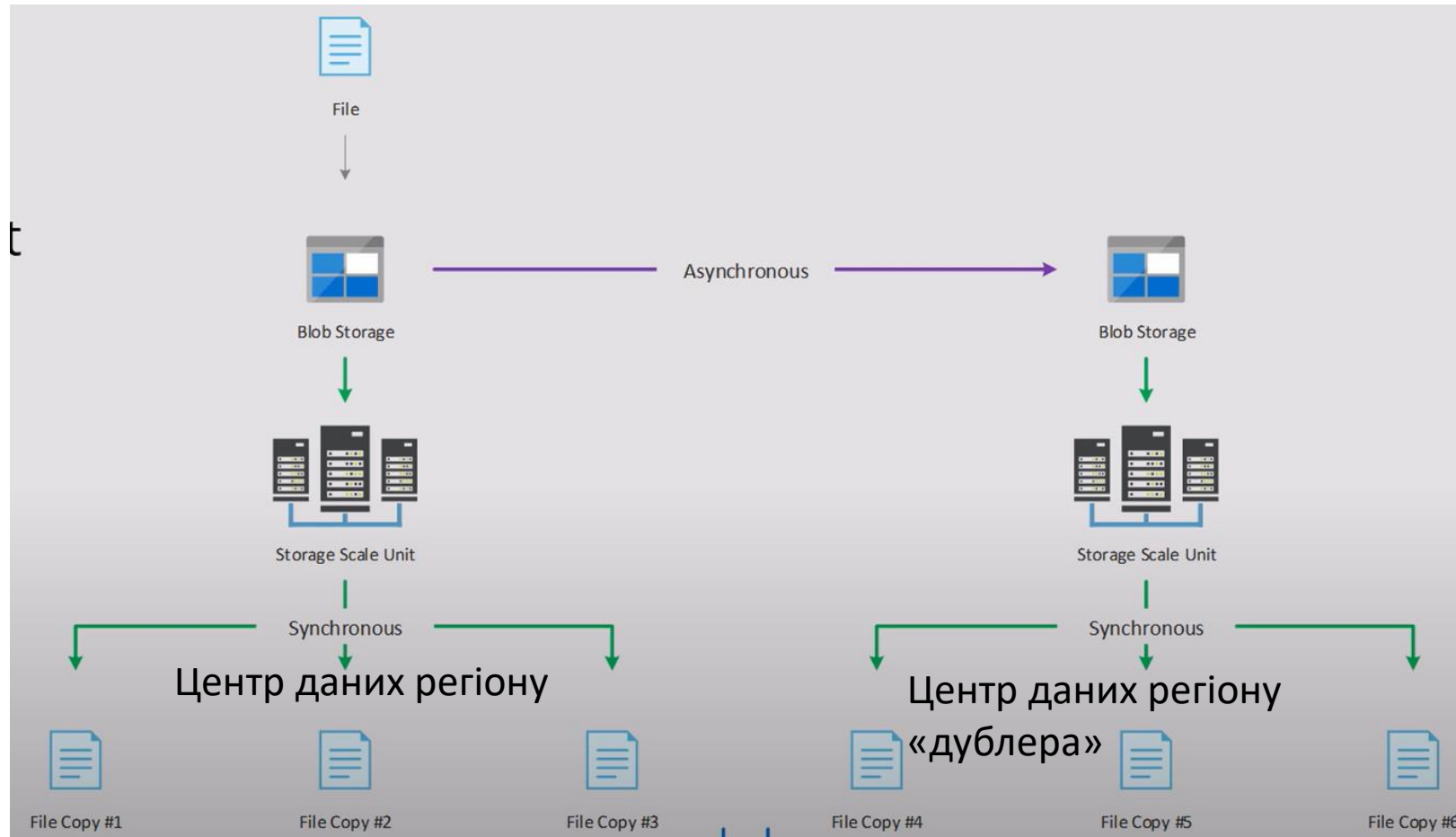
- Azure підтримує **копії** даних за наступними схемами
- Локально надлишкові дані (LRS) – дані копіюються в одному сховище.
- Надлишкові дані зони (ZRS - Zone-redundant Storage)
- Надлишкові дані в декількох регіонах (GRS - Geo-redundant storage)
- Надлишкові дані в декількох регіонах для читання (Read Access-GRS)



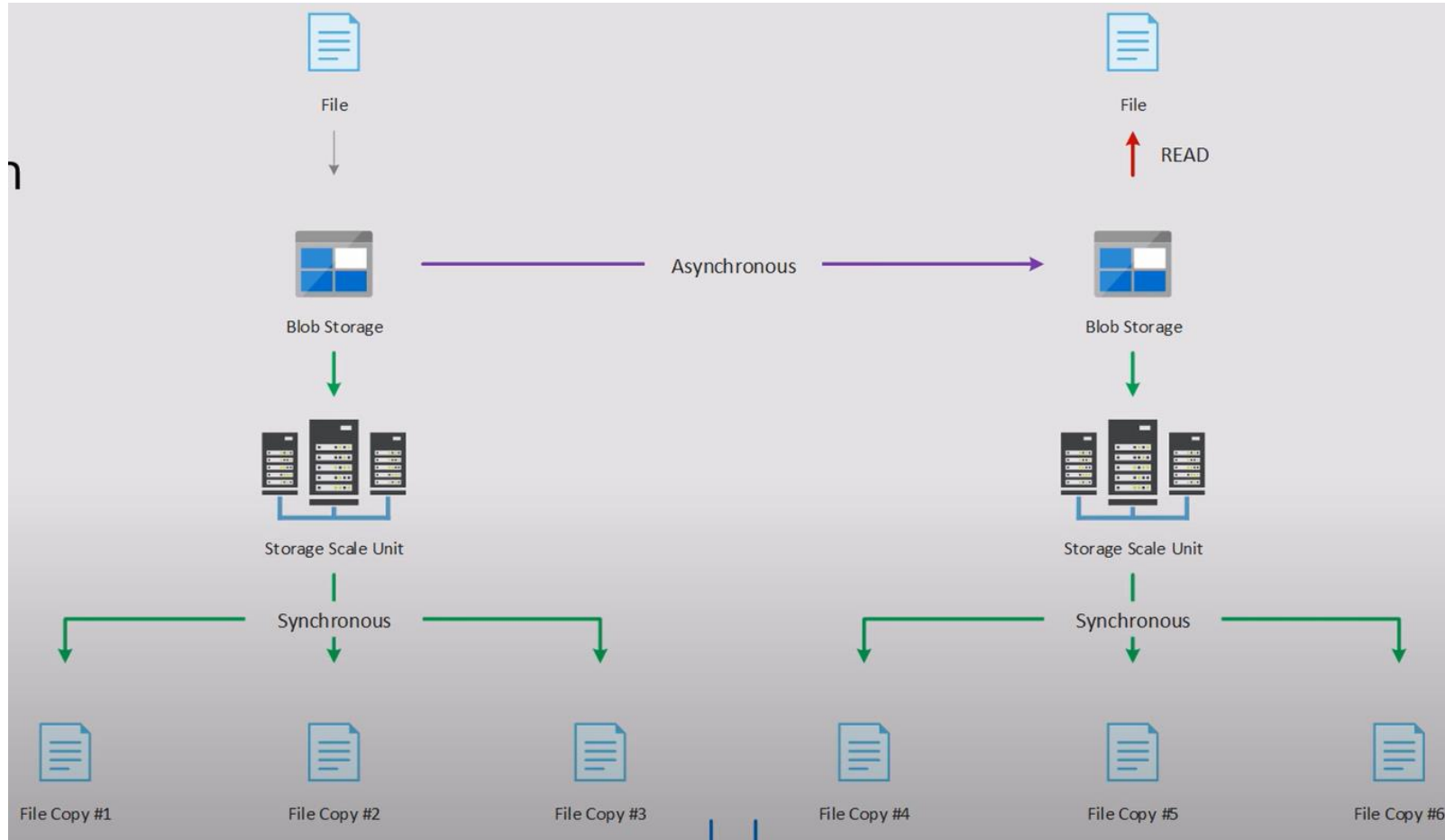
Надлишкові дані зони (ZRS - Zone-redundant Storage)
– дані копіюються синхронно по 3-х зонах доступу.



Надлишкові дані в декількох регіонах (GRS - Geo-redundant storage) – дані копіюються асинхронно в регіоні «дублере», але синхронно в файли регіону.



Надлишкові дані в декількох регіонах для читання (Read Access-GRS)–надається можливість читання даних з регіону «дублера».



Azure Blob Storage — це рішення для зберігання великих обсягів неструктурованих даних у хмарі Microsoft Azure. Воно дозволяє зберігати дані у вигляді об'єктів (blobs), таких як текстові або двійкові файли. Це популярне рішення для створення резервних копій, архівів, зберігання мультимедійних даних, а також для обробки аналітичних великих даних.

Основні компоненти Azure Blob Storage:

Storage Account (обліковий запис зберігання):

Це логічна одиниця, яка надає доступ до Azure Storage. Обліковий запис є контейнером для різних типів сховищ, включаючи Blob Storage.

Обліковий запис зберігання може використовуватися для створення і керування різними типами сховищ даних: Blob, Queue, File і Table Storage.

Він надає контроль доступу, моніторинг і управління для збережених даних.

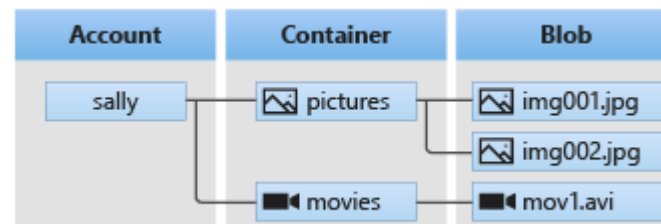
Containers (контейнери):

Контейнер є логічним екземпляром у сховищі Blob Storage, що містить групу Blob-об'єктів.

Кожний обліковий запис зберігання може містити кілька контейнерів, а кожен контейнер — необмежену кількість об'єктів (blobs).

Blobs (об'єкти):

- Це безпосередньо дані, які зберігаються в контейнері. Існує три типи blob-об'єктів:
- Block blobs: зберігають текст або двійкові дані, які ідеально підходять для зберігання великих файлів, таких як документи або мультимедіа.
- Append blobs: це варіант block blob, який призначений для запису даних у послідовному порядку, наприклад, для лог-файлів.
- Page blobs: використовуються для зберігання даних у вигляді сторінок і підходять для сценаріїв з випадковим доступом, таких як віртуальні жорсткі диски (VHD).



Основні особливості Azure Blob Storage:

Масштабованість: Azure Blob Storage дозволяє зберігати великі обсяги даних і легко масштабувати зберігання у відповідності до ваших потреб.

Гнучкість доступу: Дані можна завантажувати або зберігати через HTTP/HTTPS за допомогою API REST, SDK, або через портали Azure.

Технологія "hot", "cool" і "archive": Blob Storage підтримує різні рівні доступу:

- **Hot:** для даних, до яких часто звертаються.
- **Cool:** для даних, до яких звертаються рідко (наприклад, архіви).
- **Archive:** для даних, що рідко використовуються, але повинні зберігатися протягом тривалого періоду.

Безпека: Azure Blob Storage підтримує шифрування даних як під час передачі, так і при зберіганні. Також підтримується керування доступом за допомогою Azure Active Directory (Azure AD) і традиційних доступних токенів (Shared Access Signature, SAS).

Основні сценарії використання:

Резервне копіювання та архівування: дозволяє зберігати великі обсяги даних для резервних копій або архівів.

Зберігання великих файлів: використовується для зберігання відео, аудіо, зображень, журналів та інших мультимедійних файлів.

Хмарні додатки: для обробки великих даних і аналітичних додатків, де потрібне масове зберігання та обробка інформації.

BLOB-об'єкти Azure

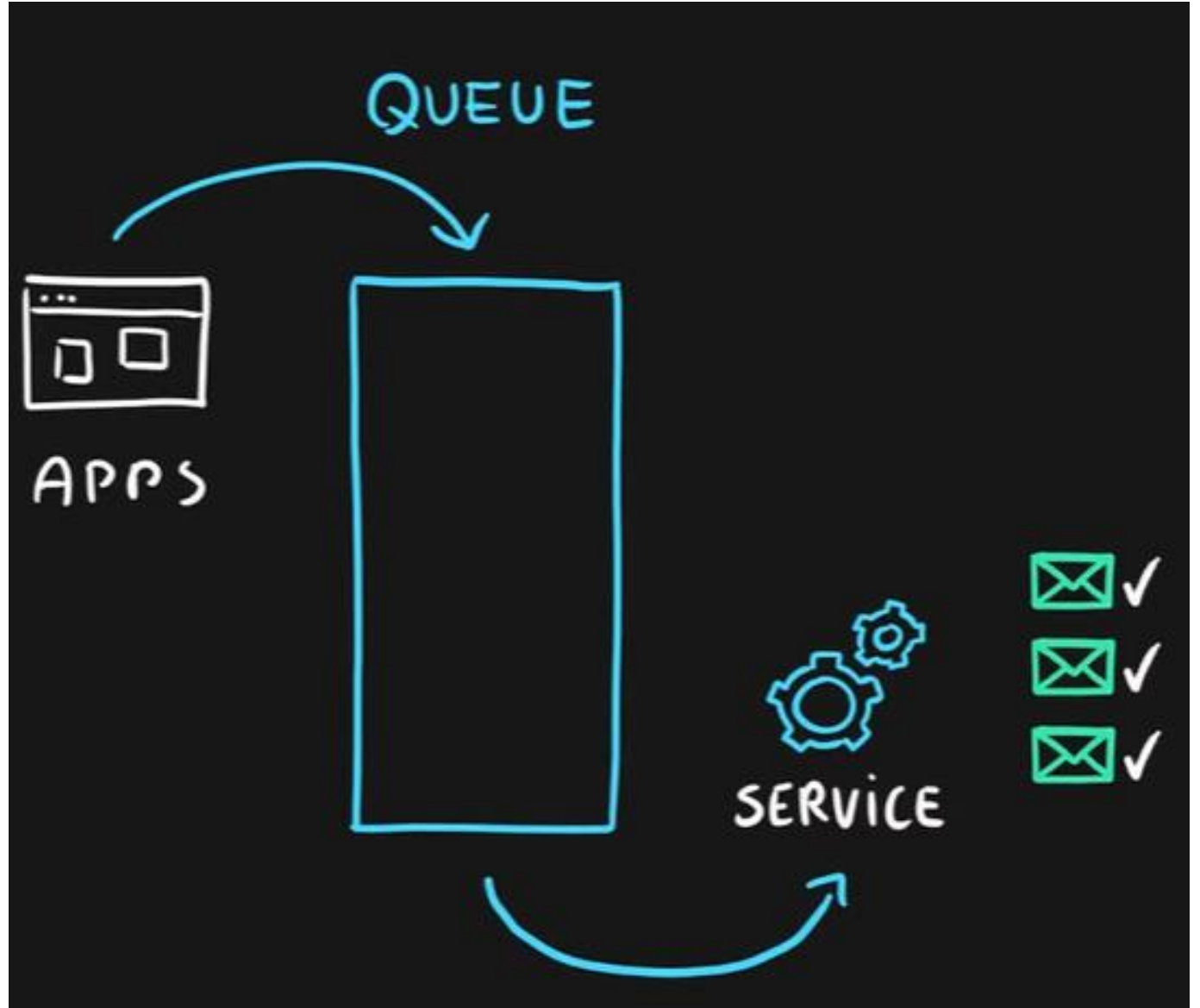
BLOB-об'єкти не обмежуються поширеними форматами файлів. BLOB-об'єкт може містити гігабайти двійкових даних.

Доступ до об'єктів у сховищі BLOB-об'єктів можна отримати з будь-якої точки світу за протоколом HTTP або HTTPS. Користувачі та клієнтські програми можуть звертатися до великих двійкових об'єктів за допомогою URL-адрес, REST API служби сховища Azure, Azure PowerShell, Azure CLI або клієнтської бібліотеки служби сховища Azure. Клієнтські бібліотеки служби сховища доступні для різних мов, у тому числі .NET, Java, Node.js, Python, PHP та Ruby.

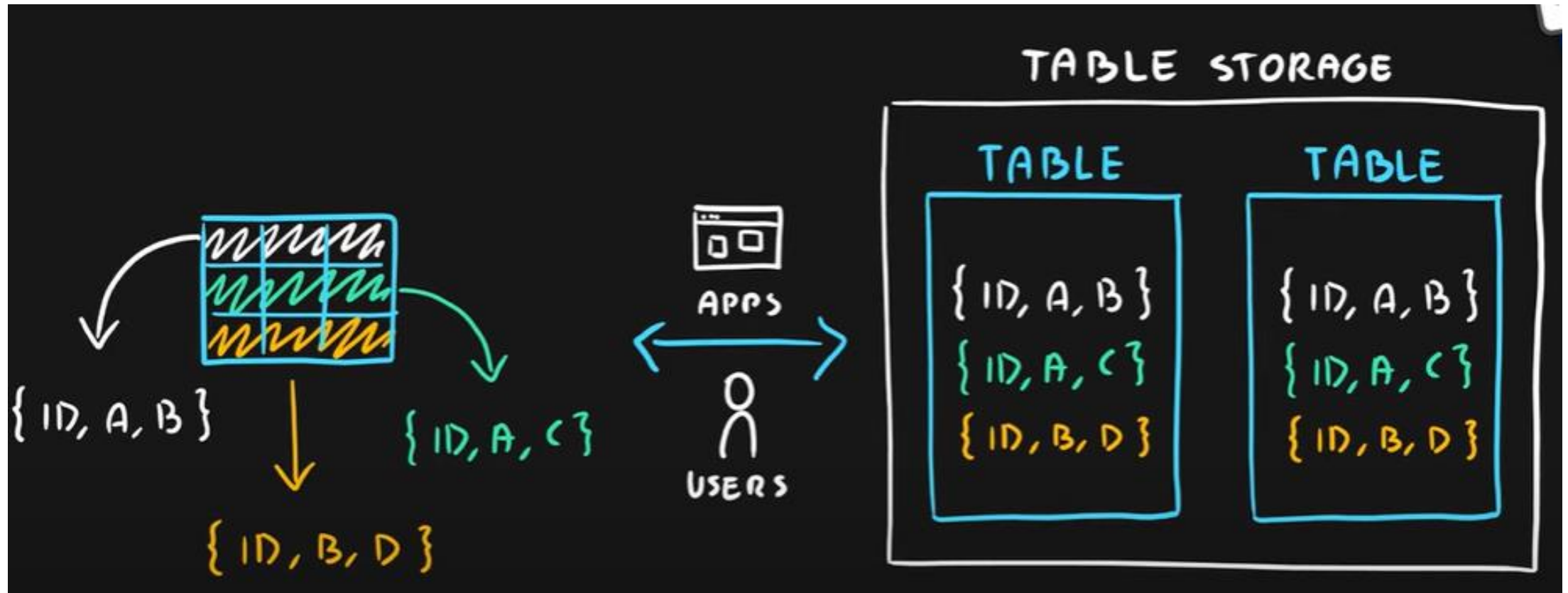
Служба сховища Azure пропонує різні рівні доступу для сховищ великих двійкових об'єктів, які забезпечують економічне зберігання об'єктів даних.

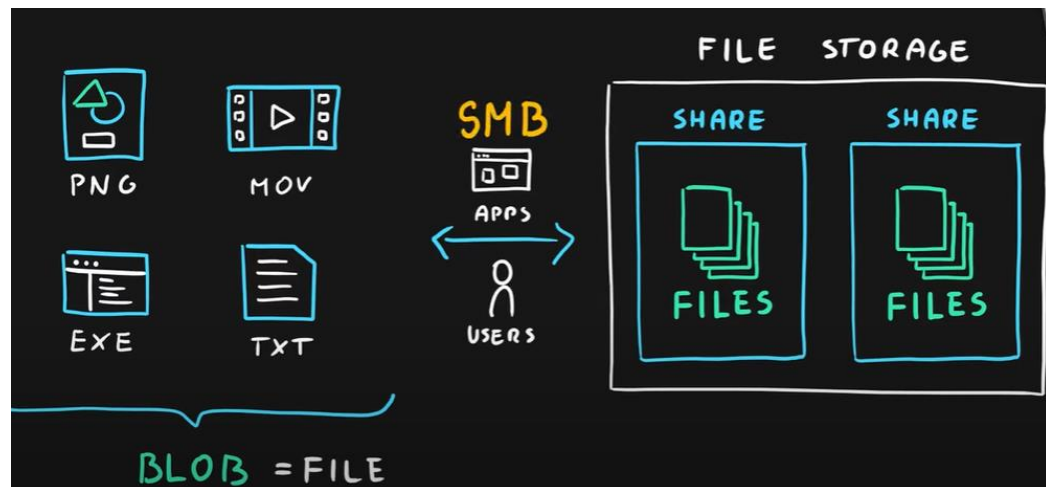
- ✓ **Гарячий рівень сховища:** Оптимізовано для зберігання даних, до яких часто звертаються (наприклад, зображення для веб-сайту).
- ✓ **Холодний рівень сховища:** Оптимізовано для даних, які використовуються нечасто та зберігаються не менше 30 днів (наприклад, рахунки для клієнтів). **Холодний рівень доступу:** оптимізовано для зберігання даних, до яких нечасто звертаються та зберігаються не менше 90 днів.
- ✓ **Архівний рівень сховища:** Призначений для даних, що використовуються нечасто та зберігаються не менше 180 днів з нестрогими вимогами до затримки (наприклад, резервні копії для довгострокового зберігання).

- Черги Azure – сховище для зберігання невеликих обсягів даних. Які необхідно асинхронно обробляти якимось процесом. Наприклад, ваш додаток має 3 задачі, яку необхідно виконати якомусь процесу, тоді ви розміщуєте ці задачі в чергу. І створюєте процес, який буде їх асинхронно обробляти.



- Таблиці Azure – сховище для зберігання напівструктурованих даних. Так дані складається в NoSQL базу даних. Для NoSQL таблиц – не можна використовувати SQL, ключі, індекси.

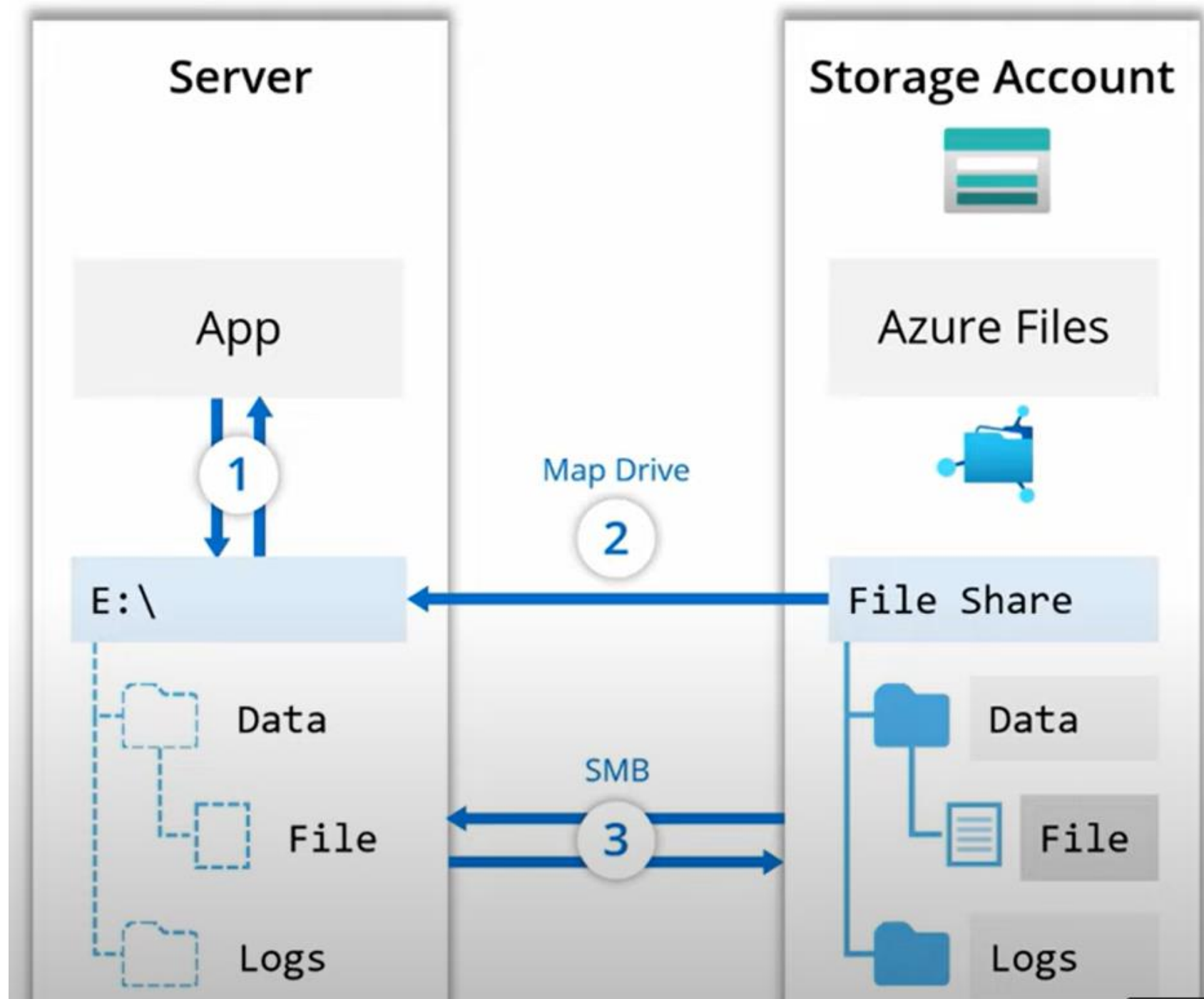




- Файлові сховища Azure мають подібну до BLOB сховищ організацію але доступ до папок з файлами отримується через SMB (**Server Message Block**) протокол
- Server Message Block (SMB) — протокол прикладного рівня (у мережевій моделі OSI), зазвичай використовується для надання розділеного доступу до файлів, принтерів, послідовних портів передачі даних, та іншої взаємодії між вузлами в комп'ютерній мережі.
- Прикладний рівень (англ. Application layer) — верхній (7-й) рівень моделі OSI, забезпечує взаємодію мережі й користувача. Саме на цьому рівні працюють всі прикладні програми, які використовують доступ до мережі, такі як оглядач вебсторінок, електронна пошта, віддалений доступ до файлів та інші. Всі протоколи рівнів нижчих за прикладний займаються доставкою даних, але корисних для кінцевого користувача функцій не надають.

Файли Azure – спосіб “lift and shift” (міграція – без внесення змін у доданок). Припустимо, на локальному сервері ви зберігаєте дані на диску E:\. Для міграції ви створюєте свій обліковий запис для збереження даних – в результаті ви отримуєте доступ до Azure файлових ресурсів. Встановлюєте відповідність між Azure папками та папками на локальному диску E:\.

SMB (Server Message Block)



Azure File Shares — це служба зберігання файлів в хмарі від Microsoft Azure, яка дозволяє створювати загальні файлові сховища для зберігання та обміну файлами в хмарному середовищі. Ця служба працює за протоколом **SMB (Server Message Block)**, що дозволяє користувачам легко мапити (монтувати) ці файлові сховища на свої локальні пристрої, подібно до локальних мережеских дисків.

Основні характеристики Azure File Shares:

1.Спільний доступ до файлів:

1. Azure File Shares надає можливість організаціям ділитися файлами між різними серверами та користувачами через мережу.

2.Протоколи:

1. Використовує SMB та NFS (для Linux середовищ) для доступу до файлів.

3.Інтеграція:

1. Легко інтегрується з Windows, Linux і macOS системами. Можна мапити файлові ресурси через стандартні засоби операційних систем.

4.Доступність:

1. Azure File Shares забезпечує високу надійність та доступність, тому файли доступні з будь-якої точки світу через Інтернет.

5.Резервне копіювання:

1. Azure забезпечує механізми для резервного копіювання файлів і відновлення їх у разі втрати.

6.Шифрування:

1. Всі дані в Azure File Shares шифруються як в стані спокою, так і під час передачі.

7.Сценарії використання:

1. Спільне використання файлів між серверами.
2. Зберігання та обмін файлами для мобільних і віддалених користувачів.
3. Інтеграція із застосунками, що потребують файлових сховищ.

Параметри облікового запису зберігання

Обліковий запис зберігання визначає політику, яка застосовується до всіх служб сховища в обліковому записі. Як приклад розглянемо наступну:

Підписка: підписка Azure, яка буде використовуватися для виставлення рахунків за служби цього облікового запису.

Розташування: Центр обробки даних, в якому зберігатимуться служби цього облікового запису.

Продуктивність: визначає, які служби даних можна використовувати у вашому обліковому записі зберігання, а також тип дисків, які використовуються для зберігання даних.

- ✓ **Стандартний:** доступні будь-які служби даних (великі двійкові об'єкти, файли, черги, таблиці); використовуються HDD-диски.
- ✓ **Преміум** надає додаткові служби зберігання даних. Наприклад, зберігання неструктурованих даних об'єкта у вигляді блокових BLOB-об'єктів або доданих BLOB-об'єктів, а також спеціальне сховище файлів, яке використовується для зберігання та створення загальних файлових ресурсів класу Преміум. Ці облікові записи зберігають накопичувачі (диски SSD).

Реплікація: визначає стратегію копіювання даних для захисту від збоїв обладнання та стихійних лих.

- ✓ Мінімальна реплікація називається локально надлишковим сховищем (LRS), що забезпечує захист від збоїв обладнання, але не від події, здатної вивести з ладу весь центр обробки даних.
- ✓ Є й більш надійна альтернатива, наприклад геонадлишкове сховище (GRS). При цьому виконується реплікація до різних центрів обробки даних по всьому світу.

Рівень доступу. Визначає, як швидко ви зможете отримати доступ до об'єктів BLOB в обліковому записі зберігання. **Гарячий рівень** доступу оптимізований для зберігання даних, до яких часто звертаються або змінюються, і забезпечує швидший доступ, ніж холодний, але з підвищеними витратами на сховище. **Холодний рівень доступу** оптимізовано для зберігання даних, до яких рідко звертаються або змінюються, і має нижчу вартість зберігання. Гарячий рівень доступу підтримує лише великі двійкові об'єкти. Він задається за замовченням для нових великих двійкових об'єктів.

Рівень доступу. Визначає, як швидко ви зможете отримати доступ до об'єктів BLOB в обліковому записі зберігання.

Hot Access Tier (Гаряче зберігання):

Призначення: Для часто використовуваних даних.

Вартість зберігання: Найвища порівняно з іншими рівнями.

Вартість доступу: Найнижча.

Типові сценарії: Використовується для даних, до яких часто звертаються або які потребують швидкого доступу, наприклад, для додатків, які виконують часті читання і запис.

Час доступу: Майже миттєвий.

2. Cool Access Tier (Прохолодне зберігання):

Призначення: Для даних, до яких звертаються рідше (1-2 рази на місяць).

Вартість зберігання: Нижча, ніж у Hot tier.

Вартість доступу: Вища, ніж у Hot tier.

Типові сценарії: Дані для довготривалого зберігання, які не часто змінюються, але їх може бути необхідно отримати без суттєвої затримки.

Наприклад, резервні копії, історичні дані.

Час доступу: Миттєвий або з мінімальною затримкою.

3. Archive Access Tier (Архівне зберігання):

Призначення: Для архівних даних, до яких звертаються дуже рідко (менше 1 разу на 6 місяців або навіть рідше).

Вартість зберігання: Найнижча серед усіх рівнів.


Вартість доступу: Найвища, оскільки необхідно "розморозувати" дані перед доступом.

Типові сценарії: Довгострокове зберігання даних для архівів, регуляторних вимог або для відновлення після катастроф. Дані зазвичай не потребують негайного доступу.

Час доступу: Вимагає декількох годин для отримання даних, після чого вони можуть бути доступні.

Розглянемо приклад доступу до файлу з рівнем доступу **Архівне зберігання**

Showing all 1 items

<input type="checkbox"/>	Name	Last modified	Access tier	Blob type	Size	Lease state	
<input checked="" type="checkbox"/>	 index.html	9/10/2024, 2:43:55 PM	Archive	Block blob	48 B	Available	...

You do not have access

Blob: index.html



This request is not authorized to perform this operation using this permission.

Summary

Session ID 4b9744a64bc84c049c9fd8c7a20a710c	Resource ID /subscriptions/601a84f6-579c-4ba6-ac84-00c597a85bd...
Extension Microsoft_Azure_Storage	Content BlobPropertiesBladeV2
Error code 403	Storage Request ID 5d747c16-b01e-0071-0481-0305c1000000

Details

- This request is not authorized to perform this operation using this permission. RequestId:5d747c16-b01e-0071-0481-0305c1000000 Time:2024-09-10T12:58:32.6882236Z
- [Learn more about authorizing access to Azure Storage](#)

Розглянемо ціни залежно від **рівеню доступу**

<https://azure.microsoft.com/en-us/pricing/calculator/>

Рішення для управління витратами – Storage Lifecycle management

Home > soloveistoredemo

soloveistoredemo | Lifecycle management



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

Storage tasks (preview)

Redundancy

Data protection

Object replication

Blob inventory

Static website

+ Add a rule ✓ Enable Disable ↻ Refresh

Lifecycle management offers a rich, rule-based policy for getting data at the end of the data's lifecycle. A new or updated policy must be applied to the data.

List View Code View

Enable access tracking ⓘ

Name

No rules

Update a rule

Details 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 haven't been modified in 15 days




Then Move to archive storage

+ Add conditions


Розглянемо приклад







Перейдемо до File shares



[Home](#) > [soloveistoredemo](#)

 **soloveistoredemo** | Storage browser   ...
Storage account

- Overview
- Activity log
- Tags
- Diagnose and solve problems
- Access Control (IAM)
- Data migration
- Events
- Storage browser**
- Storage Mover
- > Data storage
- Security + networking
 - Networking

 soloveistoredemo <

-  Favorites
- >  Recently viewed
-  Blob containers
-  File shares
-  Queues
-  Tables

 Privacy settings  Feedback

Storage account metrics

The data provided is regularly updated about 2-4 times a day and published hourly. If your account has extremely large objects, it may be over a day between updates.



Blob containers

Number of containers	-
Number of blobs	-
Total data stored	-



File shares

Number of file shares	-
Number of files	-
Total data stored	-



Tables

Number of tables	-
Number of entities	-
Total data stored	-





Queues

Number of queues	-
Number of messages	-
Total data stored	-

Завантажити файл

Home > soloveistoredemo

soloveistoredemo | Storage browser   ...
Storage account

Search

- Overview
- Activity log
- Tags
- Diagnose and solve problems
- Access Control (IAM)
- Data migration

soloveistoredemo

- Favorites
- Recently viewed
- Blob containers
- File shares
 - fileshare

[View all](#)

Upload Add directory Refresh Delete Copy Paste Rename Edit columns

File shares > fileshare

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

Search files by prefix

Showing all 4 items

<input type="checkbox"/>	Name	Type	Size
<input type="checkbox"/>	index.html	File	48 B

Створити Snapshots (знімки) для SMB File Shares

fileshare | Snapshots ...
SMB File share

Search

- Overview
- Diagnose and solve problems
- Access Control (IAM)
- Browse
- Operations
- Snapshots**

Add snapshot Refresh Delete Give feedback








<input type="checkbox"/>	Name	Date created	Initiator	Comment
<input type="checkbox"/>	2024-09-09T17:39:50.0000000Z	9/9/2024, 8:39:50 PM	Manual	demosnapshots

Одримаємо ключ для встановлення зв'язку: Storage/Data Share/FileShare/Connect







Home > soloveistoredemo | File shares >


fileshare  
SMB File share

Search

 Connect  Upload  Refresh  Add directory  Delete share  Change tier  Edit quota  Give feedback

Overview

-  Diagnose and solve problems
-  Access Control (IAM)
-  Browse
-  Operations
 -  Snapshots
 -  Backup

 Enable Backup for file share "fileshare" to protect your data. [Learn more](#)

Essentials

Storage account	: soloveistoredemo	Share URL	:
Resource group (move)	: StorageDemo	Redundancy	:
Location	: West Europe	Configuration modified	:
Subscription (move)	: Azure subscription 1		
Subscription ID	: 601a84f6-579c-4ba6-ac84-00c597a85bd9		

Properties Capabilities (2) Tutorials

Size

Maximum capacity	100 TiB
Used capacity	7.84 KiB
Tier	Cool


Performance

Maximum IO/s 	20000
Throughput rate 	Varies by region. Learn more 


Backup

Snapshots	1 snapshot
Last modified	9/9/2024, 8:39:50 PM


Feature status

Soft delete 
Large file shares

Identity-based access

Directory service 
Domain

SMB protocol settings

Security profile 
SMB protocol versions
SMB channel encryption

Connect

fileshare


To connect to this Azure file share from Windows, choose from the following authentication methods and run the PowerShell commands from a normal (not elevated) PowerShell terminal:

Drive letter

Z

Authentication method

- Active Directory or Microsoft Entra
 Storage account key

 Connecting to a share using the storage account key is only appropriate for admin access. Mounting the Azure file share with the Active Directory or Microsoft Entra identity of the user is preferred. [Learn more](#)

Hide Script

```
$connectTestResult = Test-NetConnection -ComputerName  
soloveistoredemo.file.core.windows.net -Port 445  
if ($connectTestResult.TcpTestSucceeded) {  
    # Save the password so the drive will persist on reboot  
    cmd.exe /C "cmdkey /add:"soloveistoredemo.file.core.windows.net"  
    /user:"localhost\soloveistoredemo"  
    /pass:"tKonNZVj4Jl5sGsk+Zban8TslKv5/Jm4QfIBgKBmphxvociiLSM+NAPRGF  
zEq0PJLa6pQSKmWWxv+AST9ROIIA= ""  
    # Mount the drive  
    New-PSDrive -Name Z -PSProvider FileSystem -Root  
    "\\soloveistoredemo.file.core.windows.net\fileshare" -Persist  
} else {  
    Write-Error -Message "Unable to reach the Azure storage account via port  
445. Check to make sure your organization or ISP is not blocking port 445, or  
use Azure P2S VPN, Azure S2S VPN, or Express Route to tunnel SMB traffic  
over a different port."  
}
```

Snapshots (знімки) для **SMB File Shares** в Azure використовуються для створення копій стану файлового сховища на певний момент часу. Це корисно з кількох причин:

Основні причини використання Snapshots у SMB File Shares:

1.Захист від втрати даних:

1. Знімки дозволяють відновлювати файли або цілі каталоги до попередньої версії. Якщо файл був випадково видалений або змінений, ви можете повернути його до стану, в якому він був на момент створення знімка.

2.Відновлення після збоїв:

1. Якщо відбувся збій або пошкодження даних (наприклад, через помилку користувача або програмний збій), знімки дозволяють швидко повернутися до робочого стану.

3.Історичне зберігання:

1. Знімки дозволяють зберігати історичні версії даних. Це корисно для відстеження змін у файлах і може бути частиною процесу резервного копіювання та архівування.

4.Мінімізація впливу на продуктивність:

1. Snapshots створюються миттєво і зберігаються ефективно, займаючи мало місця, оскільки записуються лише зміни з часу останнього знімка.

5.Легке відновлення без потреби в адміністраторах:

1. Користувачі можуть самостійно переглядати і відновлювати попередні версії своїх файлів за допомогою стандартного файлового менеджера (наприклад, через Windows Explorer). Snapshots інтегруються у файлову систему, що дозволяє доступ до них як до окремих версій файлів.

6.Безперервність бізнесу:

1. У разі інциденту, наприклад, кібератаки або випадкового видалення, можливість швидкого відновлення знімків гарантує безперервність роботи, мінімізуючи втрати.

Як працюють Snapshots:

- Коли створюється знімок файлового ресурсу, він фіксує стан усіх файлів та папок на даний момент.
- Після цього нові дані або зміни не перезаписують існуючі дані у знімку, а зберігаються окремо.
- Відновлення відбувається шляхом перегляду або копіювання файлів із знімка назад до основного файлового ресурсу.

Виконуємо ключ на VM – в результаті, отримуємо файли із сховища Azure доступні на віртуальній машині

The image shows a Remote Desktop Connection window titled "VM1 - 51.144.17.133:3389 - Remote Desktop Connection". Inside, a Windows PowerShell window is open, displaying the following commands and output:

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\azureuser> $connectTestResult = Test-NetConnection -ComputerName soloveistoredemo.file.core.windows.net -Port 445
PS C:\Users\azureuser> if ($connectTestResult.TcpTestSucceeded) {
  >> # Add the password so the drive will persist on reboot
  >> cmd.exe /C "cmdkey /add:"soloveistoredemo.file.core.windows.net" /user:"localhost\soloveistoredemo" /password:"tKonINZVj4J15sG5k+Zban8TsIKv5/Jm4QFI8gKBmPhxvoc1iLSM+NpRGPzeq0PJLa6pQ5KmiWxv+AST9R0IIA=" ""
  >> # Mount the drive
  >> New-PSDrive -Name Z -PSProvider FileSystem -Root "\\soloveistoredemo.file.core.windows.net\fileshare" -Persist
  >> } else {
  >> Write-Error -Message "Unable to reach the Azure storage account via port 445. Check to make sure your organization or ISP is not blocking port 445, or use Azure P2S VPN, Azure S2S VPN, or Express Route to tunnel SMB traffic over a different port."
  >> }

CMDKEY: Credential added successfully.

Name            Used (GB)  Free (GB)  Provider      Root                                     CurrentLocation
-----
Z                0.00      102400.00  FileSystem     \\soloveistoredemo.file.core.w...

PS C:\Users\azureuser> Set-Location Z:\@GMT-2024.09.17.39.50
PS Z:\@GMT-2024.09.17.39.50>
```

Below the PowerShell window, a File Explorer window is open, showing the path "This PC > fileshare (\\soloveistoredemo.file.core.windows.net) (Z:)". The File Explorer displays a table of files:

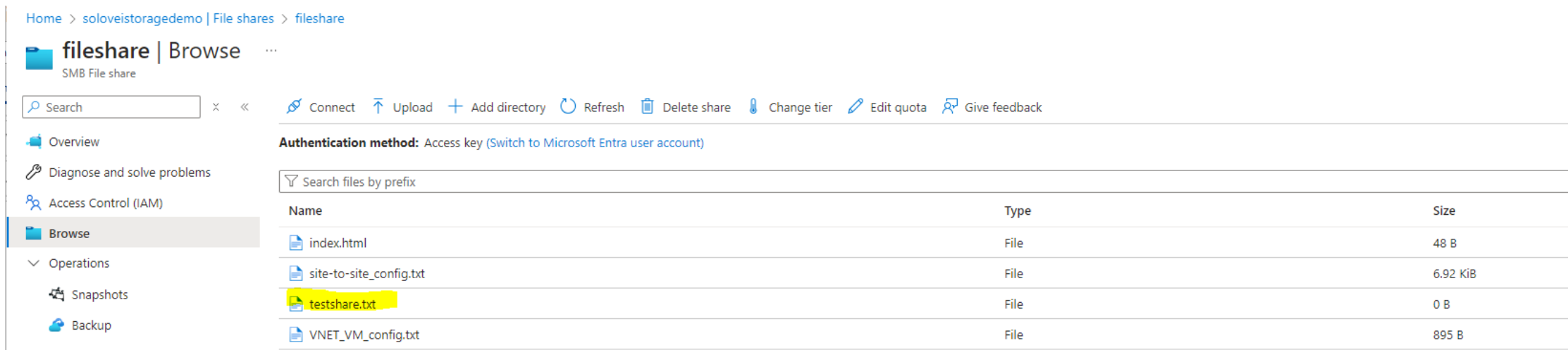
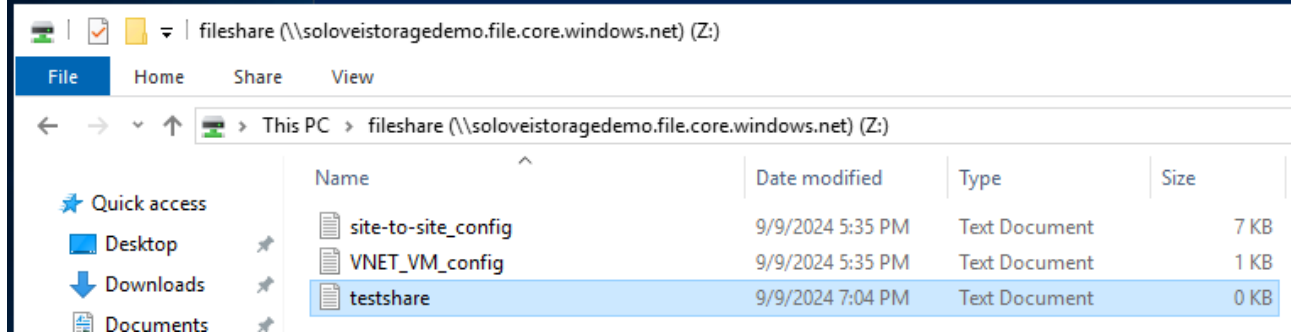
Name	Date modified	Type	Size
site-to-site_config	9/9/2024 5:35 PM	Text Document	7 KB
VNET_VM_config	9/9/2024 5:35 PM	Text Document	1 KB

Створимо файл на VM і завантажимо його в приєднану папку з файлами. Перейдемо до сховища Azure – файл буде доступний (fileshare/Browse)

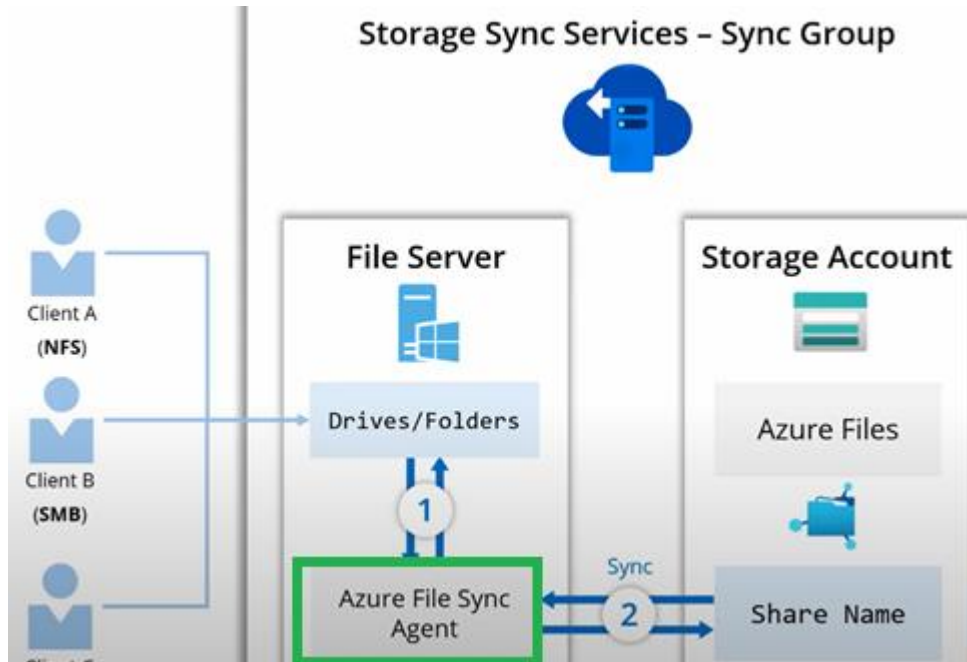
```
testshare
```

Name	Used (GB)	Free (GB)	Provider	Root
Z	0.00	102400.00	FileSystem	\\soloveistoredemo.file.core

```
PS C:\Users\azureuser> Set-Location Z:\@GMT-2024.09.09-17.39.50
PS Z:\@GMT-2024.09.09-17.39.50>
```



Azure Storage Sync — це сервіс Microsoft Azure, який дозволяє синхронізувати локальні файлові сервери з Azure File Shares, створюючи гібридне файлове сховище. Це рішення підходить для підприємств, що бажають використовувати хмарні ресурси, але при цьому зберігати файли локально.



Завдання - Синхронізація декількох серверів:

Можна синхронізувати декілька файлових серверів з одним спільним Azure File Share. Це дозволяє мати єдиний набір файлів на всіх серверах і забезпечувати доступ до них з різних локацій.

Azure Storage Sync дозволяє підприємствам інтегрувати їхні локальні файлові сервери з хмарою, без необхідності повного перенесення даних у хмару. Це зручно для організацій, що бажають зберегти локальний контроль над даними, але користуватися перевагами хмари для резервування або зменшення навантаження на локальні ресурси.

Azure File Sync Agent — це компонент, який встановлюється на локальні файлові сервери (на VM) для інтеграції з сервісом **Azure File Sync**. Він дозволяє синхронізувати дані між локальними файловими серверами та Azure File Shares, створюючи гібридне середовище для управління файлами. Основна мета агента — забезпечити постійну синхронізацію між локальним сховищем і хмарою, що дає можливість користуватися перевагами хмарних ресурсів, зберігаючи локальний доступ до файлів.

Основні функції **Azure File Sync Agent** :

Синхронізація файлів між локальним сервером і хмарою:

Storage Sync Agent дозволяє локальним файлам на файловому сервері автоматично синхронізуватися з хмарними файловими ресурсами в Azure File Share. Це забезпечує постійний зв'язок між локальною інфраструктурою і хмарою.

Кешування і Cloud Tiering:

Агент підтримує функцію cloud tiering, яка дозволяє кешувати часто використовувані файли на локальному сервері, а менш важливі файли залишаються в хмарі. Таким чином, це дає можливість оптимізувати використання локального сховища.

Мультисайтове використання:

Декілька серверів, де встановлений агент, можуть синхронізувати дані з тим самим Azure File Share, забезпечуючи єдиний набір файлів для різних локацій, що актуально для організацій із кількома офісами.

Підтримка Windows Server 2019:

StorageSyncAgent_WS2019 розроблений для роботи на Windows Server 2019, використовуючи переваги цієї версії Windows для покращеної продуктивності та безпеки під час синхронізації даних.

Захист і відновлення даних:

Агент допомагає створювати резервні копії даних в Azure та відновлювати їх у разі втрати чи пошкодження файлів на локальному сервері. Дані автоматично синхронізуються з хмарою, забезпечуючи постійне зберігання та захист.

Робота з конфліктами файлів:

Якщо два або більше серверів синхронізують один і той самий файл з різними версіями, агент вирішує ці конфлікти, використовуючи налаштовані правила або за замовчуванням, зберігаючи останню версію файлу.

Просте керування:

Після встановлення агент інтегрується з Azure Storage Sync, що дозволяє централізовано керувати всіма файлами через Azure портал, забезпечуючи моніторинг і керування процесами синхронізації.

Розглянемо приклад

•Додайте диск до VM

VM1_ | Disks

Virtual machine

Search

Refresh | Additional settings | Feedback | Troubleshoot

Warning: The configuration of this virtual machine and its attached disk(s) does not allow for the disk(s) to utilize their full throughput performance. The current virtual machine size supports 48 MBps. The total for disk(s) attached to virtual machine 'VM1_' is 125 MBps. You can change the virtual machine size to support additional disk(s) throughput. [Learn more](#)

OS disk

Swap OS disk

Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...)	Encryption ⓘ	Host caching ⓘ
VM1_disk1_d63bfcc35a964fd5aa6b7403acd65f61	Premium SSD LRS	127	500	100	SSE with PMK	Read/write

Data disks

Filter by name

Showing 1 of 1 attached data disks

+ Create and attach a new disk | Attach existing disks

LUN ⓘ	Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...)	Encryption ⓘ	Host caching ⓘ
0	Data	Premium SSD LRS	4	120	25	SSE with PMK	Read/write

Відкрити на VM – DISKmgmt

Disk Management

File Action View Help

Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(Disk 0 partition 3)	Simple	Basic		Healthy (E...	99 MB	99 MB	100 %
Temporary Stora...	Simple	Basic	NTFS	Healthy (P...	7.00 GB	6.09 GB	87 %
Windows (C:)	Simple	Basic	NTFS	Healthy (P...	126.98 GB	115.75 GB	92 %

Initialize Disk

You must initialize a disk before Logical Disk Manager can access it.

Select disks:

- Disk 2

Use the following partition style for the selected disks:

- MBR (Master Boot Record)
- GPT (GUID Partition Table)

Note: The GPT partition style is not recognized by all previous versions of Windows.

OK Cancel

Disk 0
Basic
126.98 GB
Online
450 MB

Disk 1
Basic
7.00 GB
Online
Temporary Storage (D:)
7.00 GB NTFS
Healthy (Page File, Primary Partition)

■ Unallocated ■ Primary partition

Доданий диск має статус «Unallocated». New simple Volume – визначте літеру, і відформатуйте диск

The screenshot shows the Windows Disk Management console with a 'New Simple Volume Wizard' dialog box open. The wizard is at the 'Format Partition' step, which includes the following options:

- Do not format this volume
- Format this volume with the following settings:
 - File system: NTFS
 - Allocation unit size: Default
 - Volume label: New Volume
 - Perform a quick format
 - Enable file and folder compression

The 'Next >' button is highlighted in blue. In the background, the Disk Management console shows 'Disk 2' with a 3.98 GB unallocated space, highlighted with a green border. The 'Windows (C:)' partition is also visible, showing 126.45 GB NTFS.

Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
New Simple Volume Wizard						99 MB	100 %
						6.09 GB	87 %
						115.75 GB	92 %

Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
Windows (C:)			NTFS	Healthy (Boot, Crash Dump, Primary Partition)	126.45 GB		

Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
Disk 2		Basic		Unallocated	3.98 GB		

Перевірте, що новий диск додано до VM

Disk Management

File Action View Help

Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(Disk 0 partition 3)	Simple	Basic	RAW	Healthy (E...)	99 MB	99 MB	100 %
(Disk 2 partition 2)	Simple	Basic	RAW	Healthy (P...)	3.98 GB	3.98 GB	100 %
New Volume (F:)	Simple	Basic	NTFS	Healthy (P...)	3.98 GB	3.96 GB	99 %
Temporary Storag...	Simple	Basic	NTFS	Healthy (P...)	7.00 GB	6.09 GB	87 %
Windows (C:)	Simple	Basic	NTFS	Healthy (B...)	126.45 GB	115.75 GB	92 %

Quick access

- Desktop
- Downloads
- Documents
- Pictures


This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Windows (C:)
- Temporary Storage (D:)
- New Volume (F:)**
- azurefilestorage (\\soloveistoredemo.file.core.windows.net) (Z:)
- Network

Створіть ресурс Azure File Sync

Deploy Azure File Sync ...

* Basics Networking Tags Review + create

 Storage Sync Service
Microsoft

Basics

Subscription	Azure subscription 1
Resource group	StorageDemo
Region	West Europe
Name	filesynch

Networking

Network connectivity	All networks
----------------------	--------------

Tags

(none)

Завантажте компонент для синхронізації (Azure File Sync Agent)

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

solovey.olg
КИЇВСЬКИЙ НА

Home > Microsoft.StorageSync-20240910164630 | Overview > filesynch

filesynch | Registered servers

Storage Sync Service

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
 - Network
 - Locks
 - Sync
 - Sync groups
 - Registered servers**
 - Getting Started

To register a server:

- 1 Download the [Azure File Sync agent](#) and install it on all servers you want to sync.
- 2 After finishing the agent install, use the server registration utility that opens to register the server to this Storage Sync Service. [Learn more](#)

Refresh Give feedback

Server Name	↑↓ State	↑↓ Type	↑↓ Operating System	↑↓ Agent Version	↑↓ Last seen
No items to display.					

На VM – відключити IE Enhanced Security Configuration

The screenshot shows the Windows System Information window for a virtual machine named VM1. The background window displays system details such as computer name (VM1), workgroup (WORKGROUP), last installed updates (Today at 1:34 PM), and hardware information (Intel(R) Xeon(R) Platinum 8171M CPU @ 2.60GHz, 3.45 GB RAM). A dialog box titled "Internet Explorer Enhanced Security Configuration" is overlaid on the screen. The dialog box explains that IE ESC reduces exposure to web-based attacks and is enabled by default for Administrators and Users groups. For both groups, the "Off" option is selected. The "IE Enhanced Security Configuration" text in the background window is highlighted in yellow.

Computer name: VM1
Workgroup: WORKGROUP

Last installed updates: Today at 1:34 PM
Windows Update: Install updates automatically using Windows Update
Last checked for updates: Today at 11:28 AM

Windows Defender Firewall: On
Remote management: On
Remote Desktop: On
NIC Teaming: Off

Operating system version: Windows Server 2016 Datacenter
Hardware information: Intel(R) Xeon(R) Platinum 8171M CPU @ 2.60GHz, 3.45 GB, Unknown

Processors: Intel(R) Xeon(R) Platinum 8171M CPU @ 2.60GHz
Installed memory (RAM): 3.45 GB
Total disk space: Unknown

Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.

Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.

Administrators:

- On (Recommended)
- Off

Users:

- On (Recommended)
- Off

[More about Internet Explorer Enhanced Security Configuration](#)

OK Cancel

EVENTS
All events | 4 total

Server Name	ID	Source	Message	Category	Date and Time
VM1	1002	Error	Application Hang	Application	9/10/2024 1:32:15 PM
VM1	56	Error	Application Popup	System	9/10/2024 1:07:56 PM

Maximize the everyday with Microsoft 365

Get online protection, secure cloud storage, and innovative apps designed to fit your needs—all in one plan.

For 1 person

For up to 6 people



Azure File Sync Agent

The Azure File Sync agent enables data on a Windows Server to be synchronized with an Azure File share.

Important! Selecting a language below will dynamically change the complete page content to that language.

Select language

English

Download

Choose the download you want

<input type="checkbox"/> File Name	Size
<input type="checkbox"/> Microsoft Azure File Sync - License Terms.docx	15.3 KB
<input type="checkbox"/> StorageSyncAgent_WS2016.msi	45.2 MB
<input checked="" type="checkbox"/> StorageSyncAgent_WS2019.msi	45.3 MB
<input type="checkbox"/> StorageSyncAgent_WS2022.msi	45.3 MB
<input type="checkbox"/> StorageSyncAgent_WS2012R2.msi	50.9 MB

[Download](#)

Total size: 45.3 MB

Розгорніть компонент на VM

The image shows a Windows File Explorer window with the address bar set to 'This PC > Desktop'. The left sidebar shows the 'Quick access' pane with 'Desktop' selected. The main pane displays a table of files:

Name	Date modified	Type	Size
StorageSyncAgent_WS2019			
test			

A 'Storage Sync Agent Setup' wizard window is open in the foreground. The title bar reads 'Storage Sync Agent Setup'. The main content area features a cloud icon with server racks below it and the text: 'Welcome to the Storage Sync Agent Setup Wizard'. Below this, it states: 'The Setup Wizard will install Storage Sync Agent on your computer. Click Next to continue or Cancel to exit the Setup Wizard.' At the bottom of the wizard, there are three buttons: 'Back', 'Next' (which is highlighted with a blue border), and 'Cancel'. The Microsoft Azure logo is visible in the bottom left corner of the wizard window.

Зареєструйте сервер, перевірте, що сервер з ім'ям вашої ВМ додано до ресурсу Azure File Synch/Registered servers

The image shows a Windows File Explorer window with the address bar set to `This PC > Windows (C:) > Program Files > Azure > StorageSyncAgent`. The file list contains:

Name	Date modified	Type	Size
ServerManagedIdentity.dll	6/21/2024 9:23 PM	Application extens...	14 KB
ServerRegistration	6/21/2024 9:23 PM	Application	303 KB
ServerRegistration.exe.config	6/21/2024 9:17 PM	CONFIG File	2 KB

Overlaid on the File Explorer is the **Azure File Sync - Server Registration** dialog box. It features the following elements:

- Icon:** A cloud with a server rack and arrows, representing Azure File Sync.
- Title:** "Sign in and register this server".
- Text:** "Sign in to Azure to register with an existing Storage Sync Service. To create a new Storage Sync Service, go to the Azure portal."
- Azure Environment:** A dropdown menu currently set to "AzureCloud".
- Authentication:** A toggle switch for "I am signing in as a Cloud Solution Provider" which is currently turned off.
- Action:** A blue "Sign in" button at the bottom right.

At the bottom of the File Explorer window, a status bar indicates "3 items selected 302 KB".

This PC > Windows (C:) > Program Files > Azure > StorageSyncAgent

Search StorageSyncAgent

Name	Date modified	Type	Size
ServerManagedIdentity.dll	6/21/2024 9:23 PM	Application extens...	14 KB
ServerRegistration	6/21/2024 9:23 PM	Application	303 KB
ServerRegistration.exe.config	6/21/2024 9:17 PM	CONFIG File	2 KB

tion: On
ed Universal Time
000-AA744 (activate

Azure File Sync - Server Registration

Choose a Storage Sync Service

Azure Subscription

Azure subscription 1

Subscription ID: 601a84f6-579c-4ba6-ac84-00c597a85bd9

Resource Group

StorageDemo

Storage Sync Service

filesynch

Register

age (D:)
:)
e (\soloveistoragedemo.file.core.windows.net) (Z:)

lected 302 KB



Registration successful!

✓ You can now use PowerShell or the Azure portal to configure sync.

Network connectivity test

✓ Passed. You are all set. [\(Report\)](#)

Copy Azure resource URL

Close

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
- Network
- Locks
- Sync
- Sync groups
- Registered servers**



To register a server:

- 1 Download the [Azure File Sync agent](#) and install it on all servers you want to sync.
- 2 After finishing the agent install, use the server registration utility that opens to register the server to this Storage Sync Service. [Learn more](#)

Refresh Give feedback

Server Name	State	Type	Operating System	Agent Version	Last seen
VM1	Online	Server	Windows Server 2019	18.2	9/10/2024, 5:22:45 PM

В Azure платформі створіть процедуру синхронізації

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
- Network
- Locks
- Sync
- Sync groups**

Create a sync group Refresh Give feedback

Sync group name	Status	Persistent sync errors ⓘ	Cloud endpoint
syncdemo	Healthy	0	filesharedemo

Notifications

[More events in the activity log](#) →

[Dismiss all](#) ✕




- Cloud endpoint creation succeeded**
Cloud endpoint 'filesharedemo'
2 minutes ago
- Sync group creation succeeded**
Sync group 'syncdemo'
3 minutes ago
- Successfully uploaded file(s)**
Successfully uploaded 1 file(s).
4 minutes ago

визначте диск на вашій VM дані на якому будуть синхронізовано з Azure File Share

Home > filesynch | Sync groups >

 **syncdemo**  
Sync group

 Delete sync group  Refresh  Give feedback


 Overview

> Monitoring

Monitor your sync group status

You can monitor files synced, server cache size, cache hit rate, and more here.

Server endpoints

 Add server endpoint

Server name + path	Health	Persistent sync
No items found		

Add server endpoint

A server endpoint integrates an entire volume or a subfolder of a volume from a registered server as a location to sync. The following considerations apply:

- Servers must be registered to the storage sync service that contains this sync group before you can add a location on them here.
- A specific location on the server can only sync with one sync group. Syncing the same location or even a part of it – with a different sync group doesn't work.
- Make sure that the path you specify for this server is correct.

[Learn more](#)

Registered Server *

VM1 

Path *

F:\ 


Files from this server path have been brought to the cloud via DataBox or other means of seeding the cloud endpoint (Azure file share) in this sync group.

Cloud Tiering Disabled

Initial Sync

Create

Cancel

 Give feedback

Зв'яжить локальний сервер з Azure сховищем

The screenshot shows the Microsoft Azure portal interface for a sync group named 'syncdemo'. The breadcrumb navigation is 'Home > filesynch | Sync groups > syncdemo'. The page title is 'syncdemo Sync group'. There are action buttons for 'Delete sync group', 'Refresh', and 'Give feedback'. The left sidebar shows 'Overview' and 'Monitoring' options. The main content area is divided into two sections: 'Cloud endpoint' and 'Server endpoints'. The 'Cloud endpoint' section has a table with one entry: 'filesharedemo' connected to 'soloveistoredemo' storage account, with a provisioning state of 'Provisioned' and a change enumeration completion time of 'Complete on 9/10/2024, 5:53:16 PM'. The 'Server endpoints' section has a table with one entry: 'VM1 + F:\' with a health status of 'Healthy', 0 persistent sync errors, and both upload and download operations completed on '9/10/2024' at '6:06:19 PM' and '6:06:26 PM' respectively.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > filesynch | Sync groups >

syncdemo Sync group

Search

Delete sync group Refresh Give feedback

Overview

Monitoring

Cloud endpoint

+ Add cloud endpoint

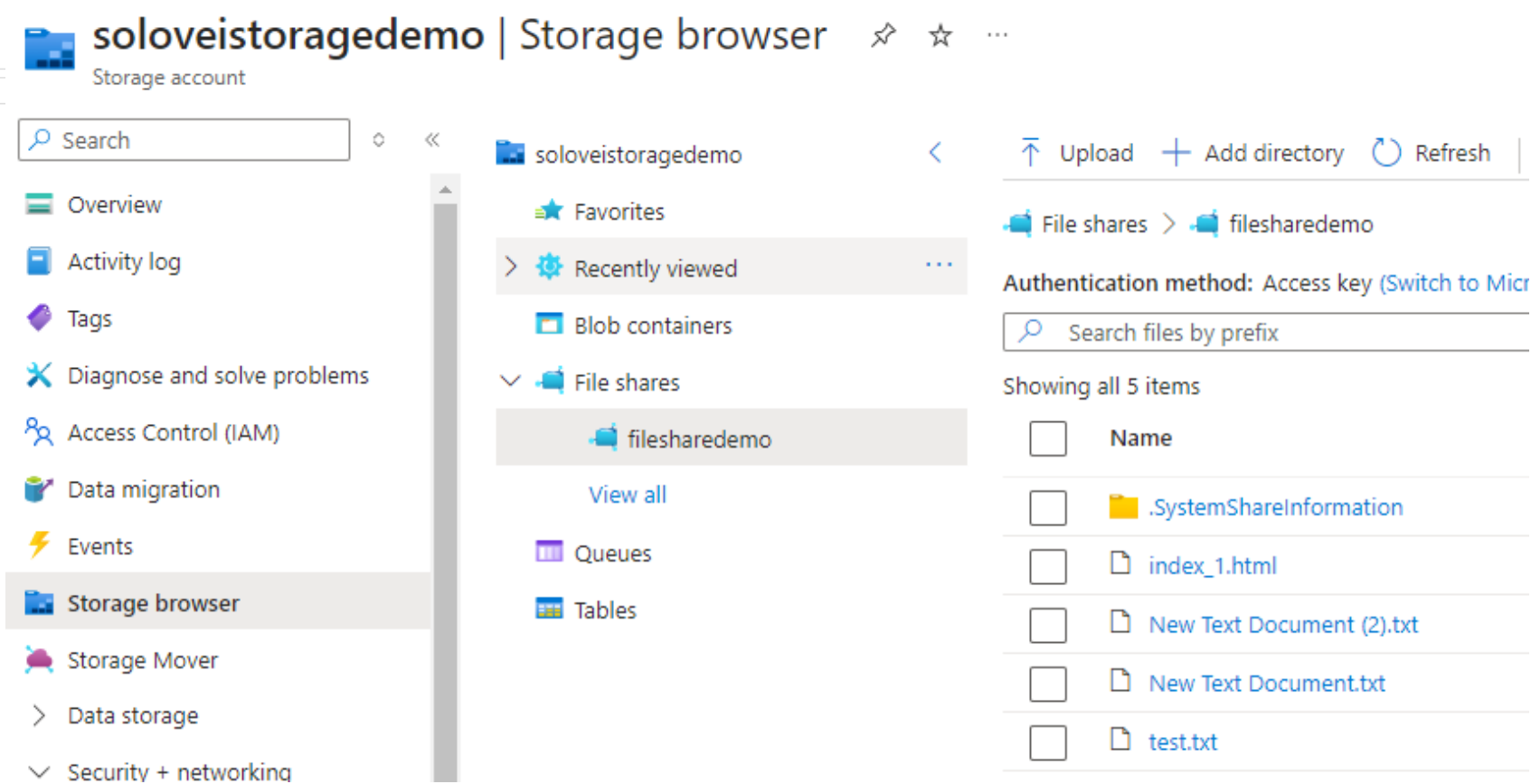
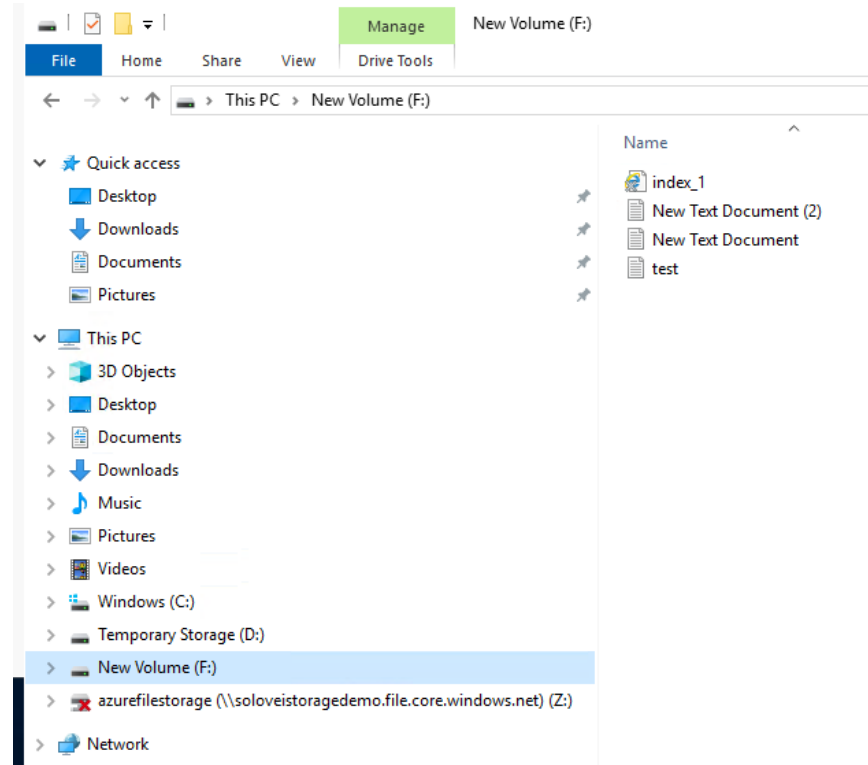
File share name	Storage account	Provisioning state	Change enumeration ⓘ
filesharedemo	soloveistoredemo	Provisioned	Complete on 9/10/2024, 5:53:16 PM

Server endpoints

+ Add server endpoint

Server name + path	Health	Persistent sync errors ⓘ	Upload to cloud	Download to server
VM1 + F:\	Healthy	0	Complete on 9/10/2024, 6:06:19 PM	Complete on 9/10/2024, 6:06:26 PM


Перевірте, що файли на локальному диску вашій VM синхронізовані з файлами в сховище Azure



клієнтська бібліотека Azure Blob Storage для Python

pip install azure-storage-blob

Home >

 **soloveistoredemo**
Storage account



Search



Essentials

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

Configuration

Data Lake Gen2 upgrade

Resource group ([move](#)) : [soloveistorage](#)

Location : westeurope

Subscription ([move](#)) : [Azure subscription 1](#)

Subscription ID : 601a84f6-579c-4ba6-ac84-00c597a85bd9

Disk state : Available

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

Performance : Standard

Replication : Locally-redundant storage (LRS)

Account kind : StorageV2 (general purpose v2)

Provisioning state : Succeeded

Created : 9/13/2024, 12:51:49 PM

Properties Monitoring Capabilities (7) Recommendations (0) Tutorials Tools + SDKs

Client libraries

Interact with Azure services using idiomatic libraries for your preferred programming languages.



.NET

Latest release: v12
Source: [GitHub](#)

[Get library](#)

[View documentation](#)



Python

Latest release: v12
Source: [GitHub](#)

[Get library](#)

[View documentation](#)



Java

Latest release: v12
Source: [GitHub](#)

[Get library](#)

[View documentation](#)



JavaScript (TypeScript)

Latest release: v12
Source: [GitHub](#)

[Get library](#)

[View documentation](#)

під час роботи з Azure Blob Storage клас `BlobServiceClient` із Azure SDK для Python надає методи для взаємодії з обліковим записом Blob Storage. ***Methods of BlobServiceClient***

1. створити контейнер

```
create_container(container_name, metadata=None, public_access=None, **kwargs)
```

2. Видалити контейнер

```
delete_container(container_name, **kwargs)
```

```
undelete_container(container_name, **kwargs)
```

3. Отримати посилання на контейнер

```
get_container_client(container)
```

```
list_containers(name_starts_with=None, include_metadata=False, **kwargs)
```


4. Отримати посилання на файл в контейнері

```
get_blob_client(container, blob)
```

5. Інформація про обліковий запис

```
get_account_information(**kwargs)
```

встановлення з'єднання з обліковим записом сховища (Storage Account)

 **soloveistoredemo** | Access keys ☆ ...
Storage account

Search

- Storage Mover
- Data storage
 - Containers
 - File shares
 - Queues
 - Tables
- Security + networking
 - Networking
 - Front Door and CDN
 - Access keys**
 - Shared access signature
 - Encryption
 - Microsoft Defender for Cloud
- Data management
- Settings
 - Configuration
 - Data Lake Gen2 upgrade
 - Resource sharing (CORS)
 - Advisor recommendations

Set rotation reminder Refresh Give feedback

Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azure Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other.

Remember to update the keys with any Azure resources and apps that use this storage account.
[Learn more about managing storage account access keys](#)

Storage account name
soloveistoredemo

key1 Rotate key
Last rotated: 9/14/2024 (0 days ago)
Key
..... Show

Connection string
..... Show

key2 Rotate key
Last rotated: 9/14/2024 (0 days ago)
Key
..... Show

Connection string
..... Show

Додайте роль – Storage Blob Data Container

Home > Azure subscription 1 | Access control (IAM) >

Add role assignment

Role **Members** Conditions Review + assign

Selected role Storage Blob Data Contributor

Assign access to User, group, or service principal
 Managed identity

Members + Select members

Name	Object ID	Type
Ольга Соловей	b16952a0-c9b6-4342-905e-fd30fa56ee85	User

Description

Optional

Home > Azure subscription 1 | Access control (IAM) >

Add role assignment

Role Members Conditions Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

× **Type : All** **Category : All**

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Defender for Storage Data Scanner	Grants access to read blobs and update index tags. This role is used by the data scanner of Defender for Storage.	BuiltInRole	None	View
Storage Blob Data Contributor	Allows for read, write and delete access to Azure Storage blob containers and data	BuiltInRole	Storage	View
Storage Blob Data Owner	Allows for full access to Azure Storage blob containers and data, including assigning POSIX access control.	BuiltInRole	Storage	View
Storage Blob Data Reader	Allows for read access to Azure Storage blob containers and data	BuiltInRole	Storage	View
Storage Blob Delegator	Allows for generation of a user delegation key which can be used to sign SAS tokens	BuiltInRole	Storage	View