

Лекція 4. Введення у сховища даних, *Azure File Shares*.

Тема 1. Створення копій стану файлового сховища для SMB File Shares.

Тема 2. Міграції “Lift and Shift” — без внесення змін до застосунку.

Тема 3. Python SDK для роботи з Azure File Share.

Тема 4. Синхронізація серверів на основі компонента Azure File Sync Agent.

Однією з найбільших переваг хмарних технологій є можливість зберігання та спільного використання файлів без необхідності керувати фізичними серверами та складною інфраструктурою. Одним із рішень, що пропонується на платформі Azure для цих цілей, є **File Shares**.

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.

- 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.

Особливість	SMB 1.0	SMB 2.0	SMB 3.0+
Рік випуску	1980-ті (Windows 95 і Windows NT)	2006 (Windows Vista/Windows Server 2008)	2012 (Windows 8/Windows Server 2012)
Швидкість	Найповільніша, низька ефективність	Покращена продуктивність, але не оптимізована для сучасних вимог	Висока швидкість, оптимізація для великих навантажень та хмарних сервісів
Безпека	Відсутність шифрування, вразливість до атак	Основні покращення безпеки, але без шифрування на рівні протоколу	Підтримка шифрування SMB3 , аутентифікація через Kerberos , захист від атак "man-in-the-middle"

```
+-----+
|  SMB 1.0 (Windows 95/NT)  |
|-----|
| - Базова підтримка клієнт-сервер |
| - Повільний, обмежена безпека   |
| - Використовувався до 2000-х років|
+-----+
```



```
+-----+
|  SMB 2.0 (Windows Vista/2008) |
|-----|
| - Покращена швидкість і безпека |
| - Підтримка більших кешів       |
| - Оптимізація для локальних мереж|
+-----+
```



```
+-----+
|  SMB 3.0+ (Windows 8/2012+)  |
|-----|
| - Висока швидкість та масштабованість|
| - Підтримка шифрування (SMB3)   |
| - Ідеально підходить для хмарних рішень|
+-----+
```

SMB 1.0:

Початковий протокол, який забезпечував базову функціональність для спільного доступу до файлів і принтерів, але мав багато обмежень у продуктивності та безпеці.

SMB 2.0:

Протокол SMB 2.0 був значно покращений. Він збільшив швидкість роботи, зменшив витрати на мережеві ресурси і підтримував більші файли, але не мав шифрування на рівні протоколу.

SMB 3.0+

Введений у Windows 8 і Windows Server 2012, SMB 3.0 забезпечує високу продуктивність і надійність, підтримку шифрування даних, а також оптимізацію для великих масштабів і хмарних рішень. Ця версія стала стандартом для сучасних корпоративних мереж.

Особливість	SMB 1.0	SMB 2.0	SMB 3.0+
Підтримка великих файлів	Обмеження на максимальний розмір файлу	Підтримка більших файлів, але без оптимізації	Можливість роботи з величезними файлами, великі можливості для великих даних
Технології та функції	Малі можливості для багатозадачності та масштабованості	Підтримка більших розмірів кешів, значне покращення при роботі з мережами	Додаткові функції: ліцензування через SMB Direct, компресія даних, підтримка журналістики для файлів
Мобільність та адаптивність	Низька ефективність у великих мережах	Покращена мобільність та масштабованість	Підтримка хмар та оптимізація для віддалених мереж
Використання	В основному для локальних мереж і старих систем	Для підприємств, середовище з більшою вимогою до ефективності	Для сучасних підприємств, хмарних рішень, з високими вимогами до безпеки і ефективності
Підтримка відмовостійкості	Обмежена підтримка наявності резервних шляхів	Покращена підтримка при відмовах і відновленнях	Висока відмовостійкість через додаткові можливості (наприклад, відновлення після аварії)

Ключові слова

Поняття	Опис
Share	Верхній рівень файлового сховища. Наприклад: \\myaccount.file.core.windows.net\myshare
Directory	Папка у сховищі — може містити підпапки та файли (аналог папок у провіднику).
File	Стандартний файл будь-якого типу (документ, скрипт, тощо).

Локальна мережа	Azure Files
Мережевий диск H:	Хмарне сховище *.file.core.windows.net*
Протокол SMB	Той самий SMB
Файли на сервері в універі	Файли в хмарі Microsoft Azure

Що таке спільні мережеві диски?

Це файлові сховища, до яких можуть одночасно підключатися кілька користувачів або серверів у мережі.

Azure Files — це хмарний сервіс Microsoft Azure для зберігання файлів, який:

Працює як спільний мережевий диск, але у хмарі.

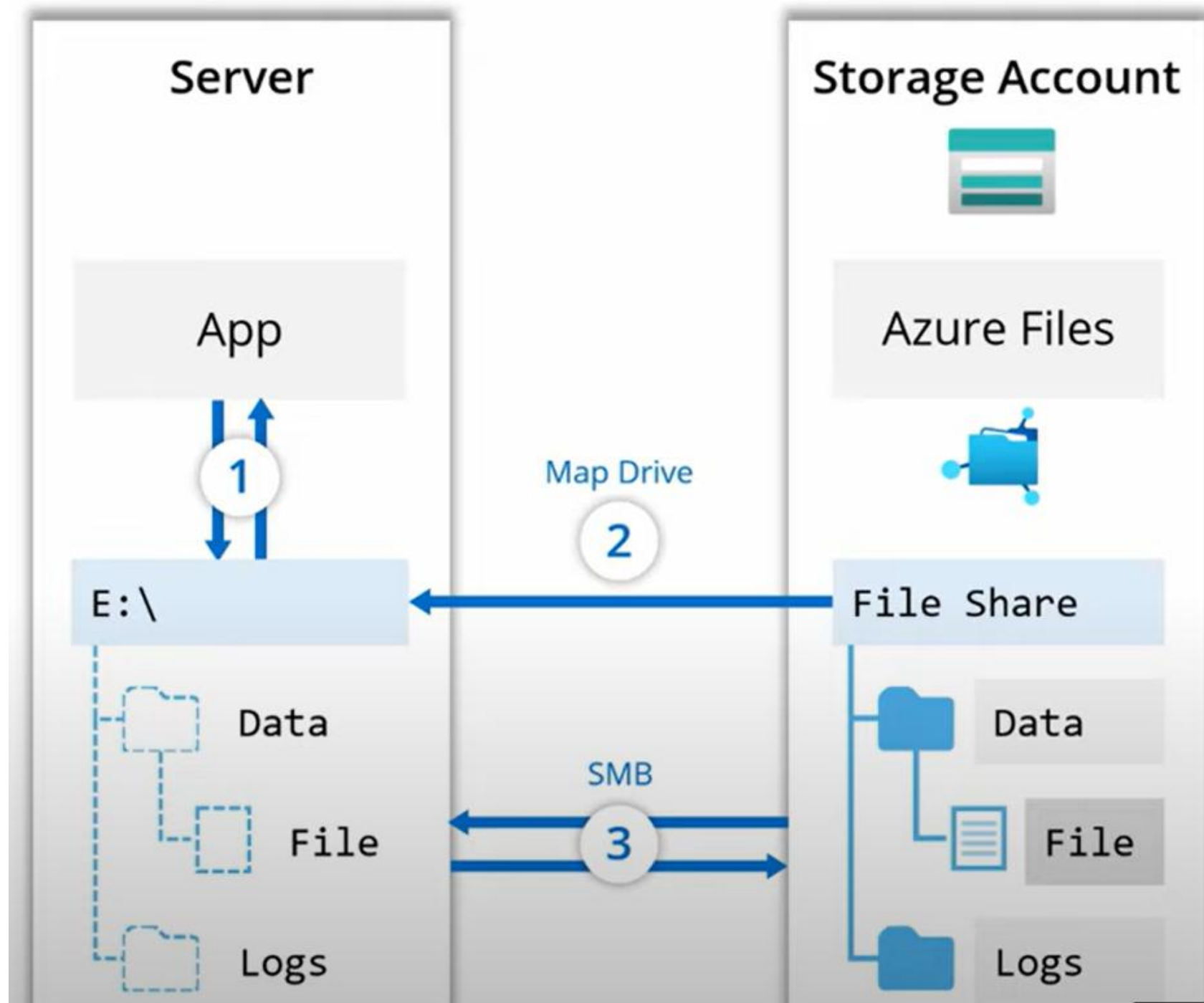
Повністю керований: не потрібно налаштовувати власні файлові сервери.

Основні сценарії використання - "Lift and Shift" міграції

- ✓ Перенесення застарілих додатків у хмару без змін у коді.
- ✓ Особливо корисно, якщо додатки використовують файлові шляхи, які не можна змінити.
- ✓ Спільне використання конфігураційних файлів - Можна зберігати налаштування, які використовують кілька віртуальних машин.
- ✓ Централізоване зберігання - Збереження логів, інструментів розробки, скриптів, загальних ресурсів.

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)



Завантажити файл в створений ресурс типу.

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

UploadAdd directoryRefreshDeleteCopyPasteRenameEdit columns

File shares > fileshare

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

Search files by prefix

Showing all 4 items

	Name	Type	Size
	index.html	File	48 B

Створити Snapshots (знімки) для SMB File Shares

fileshare | Snapshots

SMB File share

Search

+ Add snapshotRefreshDeleteGive feedback

Overview

Diagnose and solve problems

Access Control (IAM)

Browse

Operations

Snapshots

	Name	Date created	Initiator	Comment
	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

×

«

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

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

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+Zban8TsIKv5/Jm4QfIBgKBmphxvociiLSM+NAPRGFzEq0PJLa6pQSKmWWxv+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."
}
```

Ключ – це код на PowerShell призначений для підключення до **Azure File Share** через SMB-протокол, а також для збереження облікових даних і підключення до файлового шару, щоб він був доступний навіть після перезавантаження комп'ютера.

Test-NetConnection

- **Test-NetConnection** — це команда PowerShell, яка перевіряє наявність з'єднання з певним комп'ютером або сервісом через зазначений порт.
 - **-ComputerName** вказує на адресу, до якої потрібно підключитися. У цьому випадку це адреса вашого **Azure Storage Account**.
 - **-Port 445** вказує порт, на якому буде здійснена перевірка. Порт 445 — це стандартний порт для **SMB** (Server Message Block), який використовується для доступу до файлів на сервері.
- Змінна **\$connectTestResult** збереже результат цієї перевірки: чи вдалося підключитися до сервісу на порту 445.

```
$connectTestResult = Test-NetConnection -ComputerName soloveistorageaccount.file.core.windows.net -Port 445
```

Перевірка результату підключення

Умова перевіряє, чи вдалося встановити TCP-з'єднання через порт 445. Якщо **Test-NetConnection** повернув результат, що з'єднання успішне, код всередині умови буде виконано.

```
if ($connectTestResult.TcpTestSucceeded) {
```

Збереження облікових даних за допомогою cmdkey

cmdkey — це інструмент, що дозволяє зберігати облікові дані для доступу до мережевих ресурсів.

/add — додає нові облікові дані.

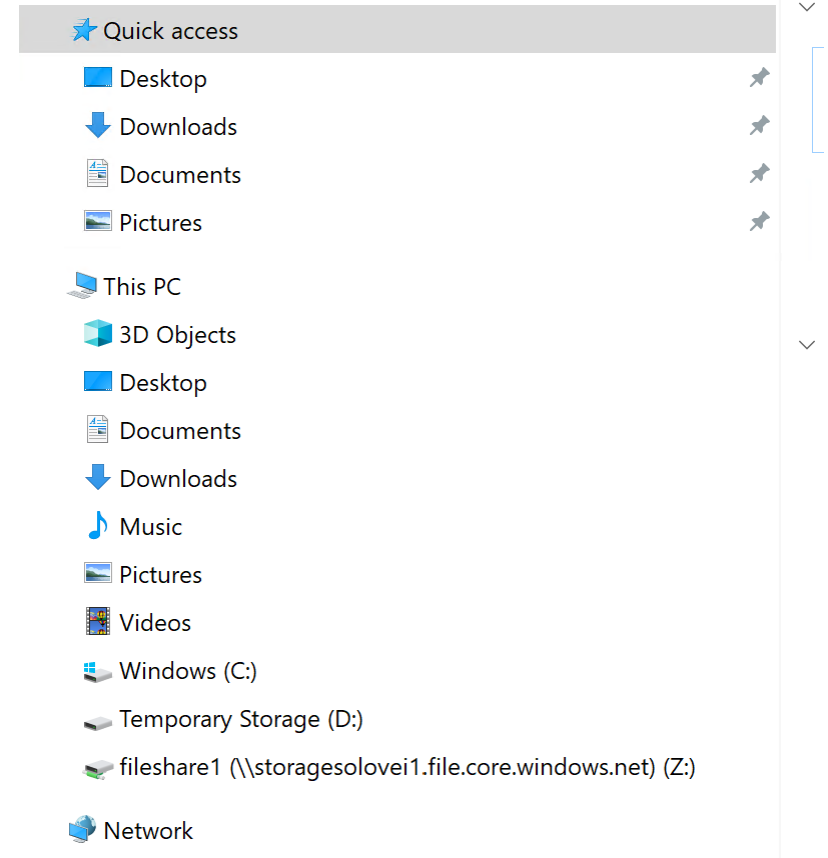
/user — вказує ім'я користувача для підключення. Тут це користувач з форматом localhost\soloveistorageaccount, що означає, що для доступу використовується локальний обліковий запис, що відповідає обліковому запису Azure File Share.

/pass — пароль, що використовується для доступу.

```
cmd.exe /C "cmdkey /add:"soloveistorageaccount.file.core.windows.net"  
/user:"localhost\soloveistorageaccount"  
/pass:"RA/tc40piJBr4PgTwxf1ZVsfVm59p2ZrPrWwolOyFEZOqV5+q+DShHcVTBybV0WYJU9m6XzzTnJW+AStDqUw5  
Q=="""
```

Підсумок - ключ PowerShell здійснює кілька важливих кроків для підключення до **Azure File Share** через SMB:

- 1.Перевіряє з'єднання з Azure Storage Account через порт 445.
- 2.Якщо з'єднання успішне, зберігає облікові дані для підключення до SMB файлового шару.
- 3.Монтує файловий шар як новий диск **Z**.
- 4.Якщо підключення не вдалося, виводить помилку.
- 5.Змінює робочу директорию на певну папку на змонтованому диску.



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

VM1 - 51.144.17.133:3389 - Remote Desktop Connection

Recycle Bin
Microsoft Edge

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) {
 >> I have 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/Jm4QFI8gKBmPhxvocilLSH+NApRGfzEq0P3La6pQ5KmiWxv+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."
 >> }

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-2024.09.09-17.39.50
PS Z:\@GMT-2024.09.09-17.39.50>

File

Home

Share

View

Drive Tools

Manage

fileshare (\\soloveistoredemo.file.core.windows.net) (Z:)

←

→

⌵

⬆

🖥

>

This PC > fileshare (\\soloveistoredemo.file.core.windows.net) (Z:)

Quick access

Desktop

Downloads

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>
```

fileshare (\\soloveistoredemo.file.core.windows.net) (Z:)

FileHomeShareView

Quick access

Desktop

Downloads

Documents

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
testshare	9/9/2024 7:04 PM	Text Document	0 KB

Home > soloveistoredemo | File shares > fileshare

fileshare | Browse

SMB File share

Search

ConnectUploadAdd directoryRefreshDelete shareChange tierEdit quotaGive feedback

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

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

Search files by prefix

Name	Type	Size
index.html	File	48 B
site-to-site_config.txt	File	6.92 KiB
testshare.txt	File	0 B
VNET_VM_config.txt	File	895 B

Azure Storage File Share client library for Python - version 12.22.0 (pip install azure-storage-file-share)

імпорт класу ShareServiceClient із пакету
azure.storage.fileshare
Створення клієнта служби: URL до файлової
служби вашого Storage Account. Облікові дані
(ключ доступу, токен, або об'єкт
DefaultAzureCredential) для автентифікації.
Об'єкт ShareServiceClient, який надає
можливість:
переглядати наявні File Shares;
створювати або видаляти File Shares;
отримувати доступ до директорій і файлів;
виконувати інші дії на рівні файлового сервісу.

```
from azure.storage.fileshare import  
ShareServiceClient  
  
service =  
ShareServiceClient(account_url="https://<my-  
storage-account-name>.file.core.windows.net/",  
credential=credential)
```

Створити SAS-токен (Shared Access Signature)

створити SAS-токен (Shared Access Signature) для доступу до Azure File Share та підключитися до нього з обмеженими правами доступу.

Параметр Значення / Призначення

account_name- Назва вашого Storage Account

account_key- Один із ключів доступу до Storage Account

resource_types - Вказує, до яких типів ресурсів надається доступ:

Наприклад, service=True означає доступ до сервісного рівня (тобто самого File Share)

permission- Дозволи, які надає SAS-токен:

read=True — тільки читання

expiry Час закінчення дії токена: через 1 годину від поточного UTC часу

```

sas_token = generate_account_sas(
    account_name="<storage-account-name>",
    account_key="<account-access-key>",
    resource_types=ResourceTypes(service=True),
    permission=AccountSasPermissions(read=True),
    expiry=datetime.utcnow() + timedelta(hours=1)
)

```

4 різні клієнти (класи) в Python SDK *azure.storage.fileshare*, які надають доступ до різних рівнів ієрархії Azure File Share.

Отримувати список усіх File Share'ів у сховищі. Створювати або видаляти File Share. Налаштовувати властивості сервісу.	ShareServiceClient get_share_client("myshare")
Створити, видалити, налаштувати або створити snapshot для File Share. Переглядати або створювати директорії всередині File Share. Отримувати клієнтів для директорій або файлів:	ShareClient get_directory_client("mydir") get_file_client("mydir/myfile.txt")
Створювати, видаляти директорії. Переглядати вміст директорії (файли та підкаталоги). Створювати файли або вкладені підкаталоги.	ShareDirectoryClient get_file_client("file.txt") get_subdirectory_client("nested_dir")
Завантажувати (upload), створювати, видаляти файл. Копіювати файл між директоріями або File Share'ами. Працювати напряду з вмістом файлу	ShareFileClient upload_file(open("localfile.txt", "rb")) download_file()

Клас

Доступ до...

ShareServiceClient

**Усі File Share'и в
акаунті**

ShareClient

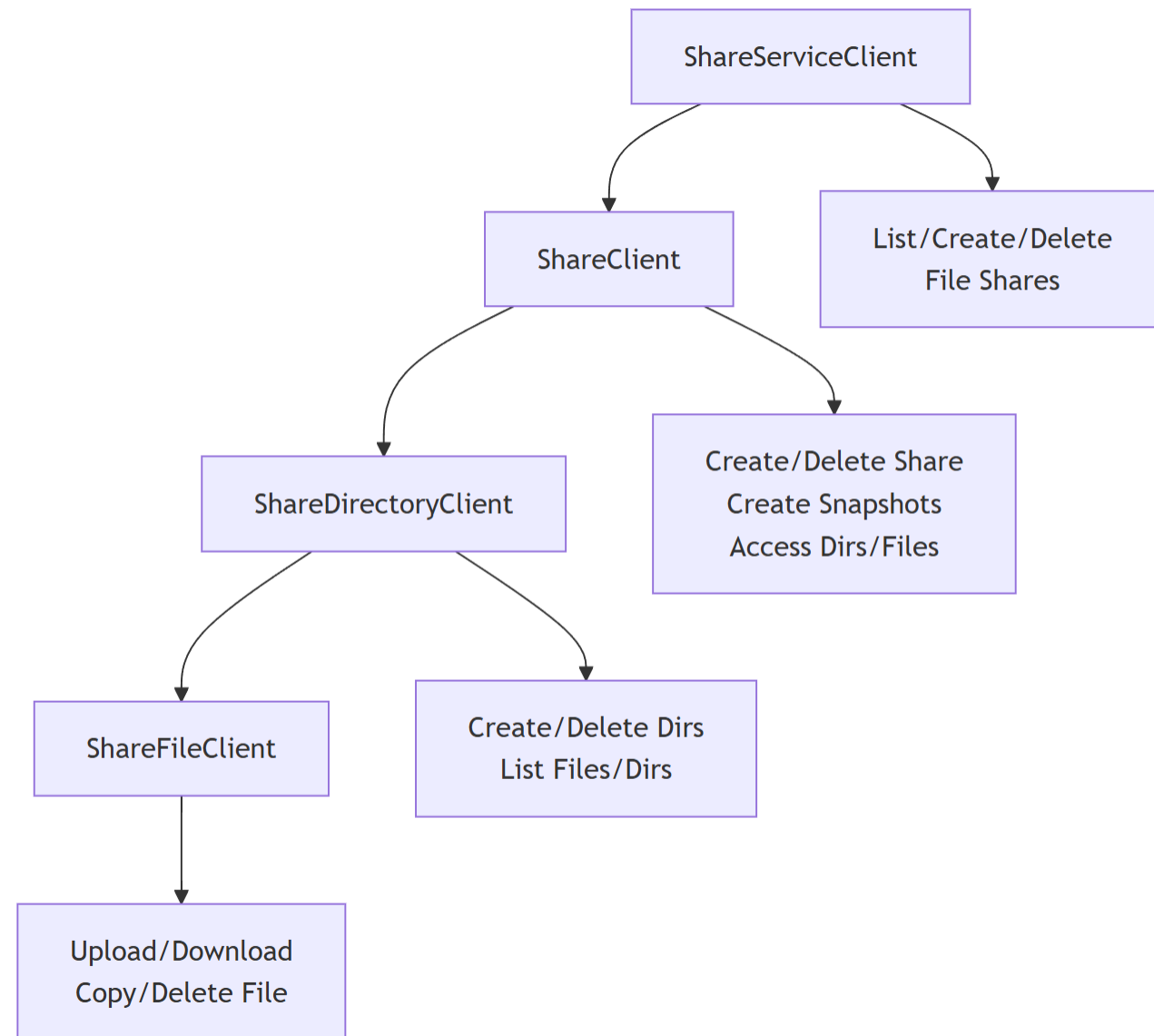
**Один конкретний
File Share**

ShareDirectoryClient

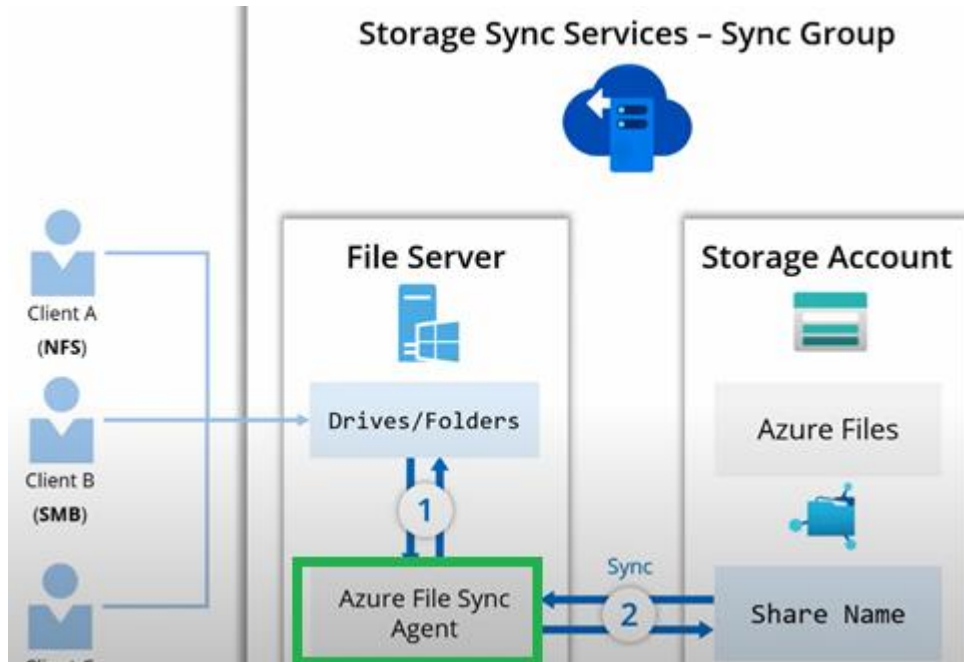
**Певна директорія в
Share**

ShareFileClient

**Один конкретний
файл**



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.

•**Локальні файли:** Це файли, які часто використовуються або змінюються. Вони зберігаються на локальному сервері.

•**Хмарні файли:** Це файли, які рідко використовуються або не були відкриті в певний період часу. Вони переміщуються в хмару, і доступ до них здійснюється на запит (тобто, вони можуть бути завантажені з Azure при потребі).

✓ 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.

Azure File Sync — це сервіс, який дозволяє синхронізувати файли між **локальним файловим сервером** (або віртуальною машиною) і **Azure File Share**. Щоб запустити процес синхронізації, необхідно створити **Server Endpoint** — точку підключення, яка вказує на конкретну локальну папку.

Server Endpoint — це шлях до локальної папки (на вашому сервері або VM), яка буде синхронізуватися з Azure File Share через сервіс Azure File Sync.

Умови створення Server Endpoint:

Умова	Пояснення
Зареєстрований сервер	Endpoint повинен бути створений на зареєстрованому сервері (через File Sync Agent)
NAS не підтримується	Мережеві шляхи не можна використовувати як endpoint
Cloud Tiering обмежений	Не працює на C:\ (системному томі)
Незмінний шлях	Неможна змінювати шлях або диск після створення
Один endpoint на Sync Group	Один сервер = один endpoint в межах однієї Sync Group
Кілька endpoint'ів — дозволено	Але лише з різними Sync Groups і не перекриваючими шляхами

Основні умови створення Server Endpoint

Агент встановлюється на локальному сервері або віртуальній машині, яка буде брати участь у синхронізації.

Після встановлення необхідно зареєструвати сервер у відповідному Storage Sync Service.

Створений ресурс Storage Sync Service у Azure - це основний сервіс у хмарі, який:

зв'язує локальні сервери з Azure File Share, керує синхронізацією, обробляє конфлікти та метадані.

Sync Group — це логічна група, яка об'єднує: один Azure File Share, і один або більше Server Endpoint'ів.

Усі Server Endpoint'и у Sync Group синхронізуються між собою та з хмарним сховищем.

Для обміну даними з Azure використовується порт 443 (HTTPS).

Умова	Значення
Azure File Sync Agent встановлений	Без агента синхронізація неможлива
Зареєстрований сервер	Підключений до Azure
Створено Storage Sync Service	Керує синхронізацією
Створено Sync Group	Об'єднує File Share і Endpoint
Сервер має доступ до Azure	Порт 443 повинен бути відкритим
Дотримано обмежень масштабування	Не перевищено кількість endpoint'ів і обсягів

Cloud Tiering — це функція Azure File Sync, яка дозволяє **автоматично переміщати рідко використовувані файли з локального сервера в Azure File Share**, зберігаючи при цьому лише **метадані (ім'я, розмір, атрибути)** файлів на диску. Файли залишаються доступними локально, але фактично зберігаються в хмарі.

Додати диск до VM на платформі Azure

 Search





-  Activity log
-  Access control (IAM)
-  Tags
-  Diagnose and solve problems
-  Resource visualizer
-  Connect
-  Networking
-  Network settings
-  Load balancing
-  Application security groups
-  Network manager
-  Settings

OS disk

 Swap OS disk

Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...)	Encryption ⓘ
VM1_OsDisk_1_8f3a335065ce420d8dec	Premium SSD LRS	127	500	100	SSE with PMK

Data disks

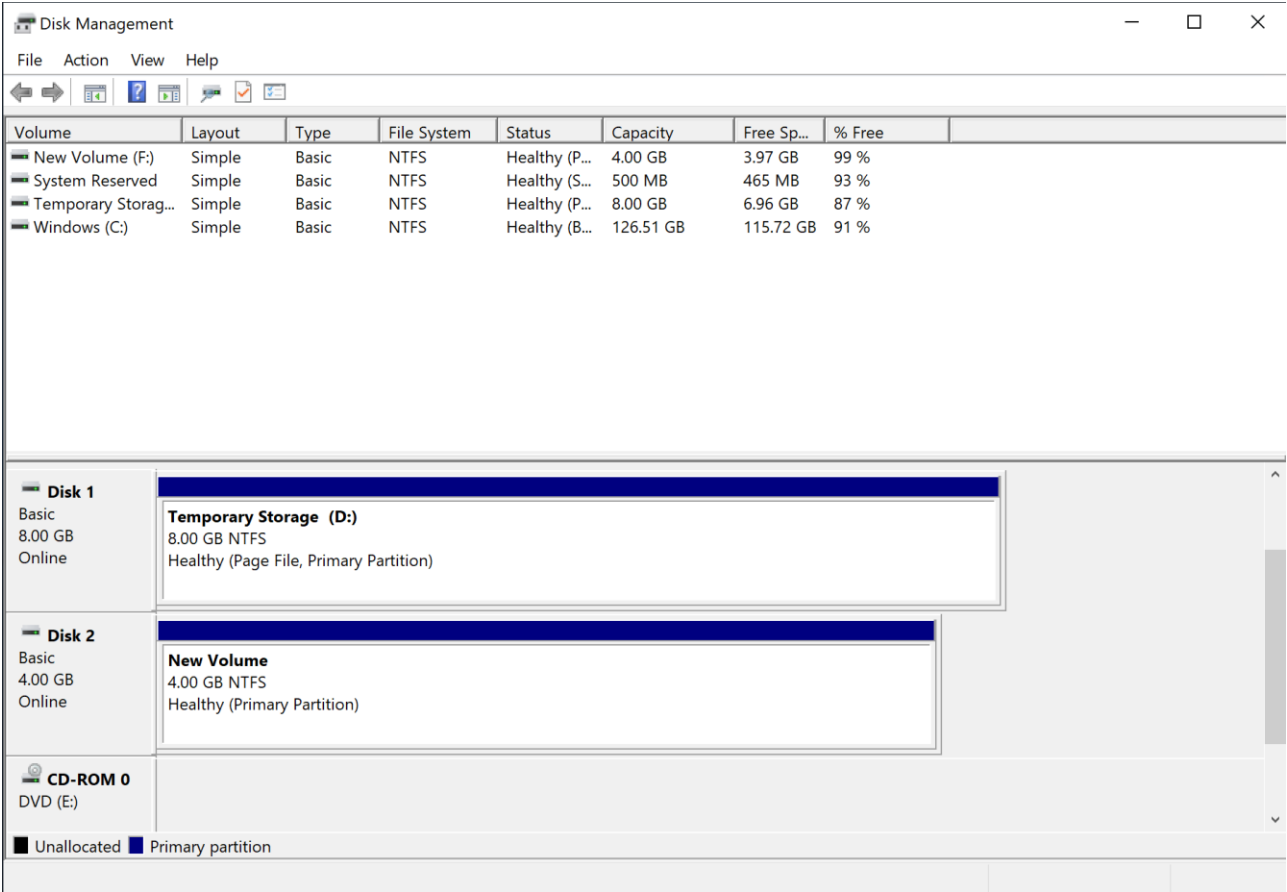
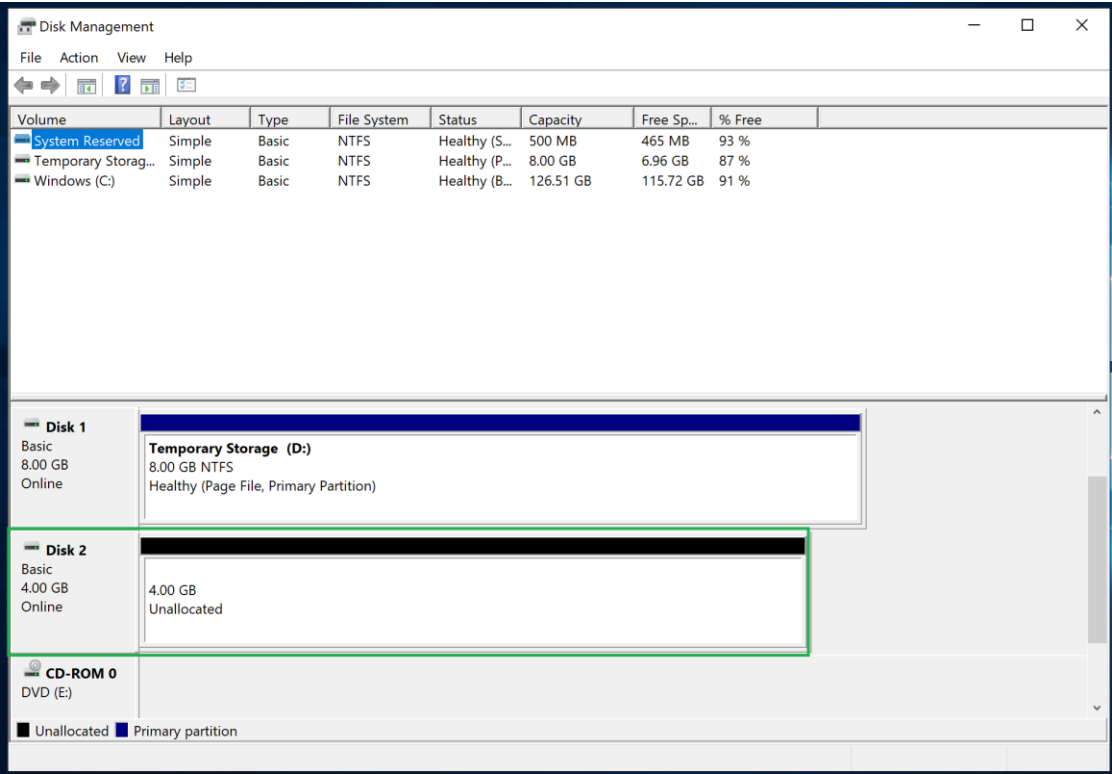
 Filter by name

Showing 1 of 1 attached data disks

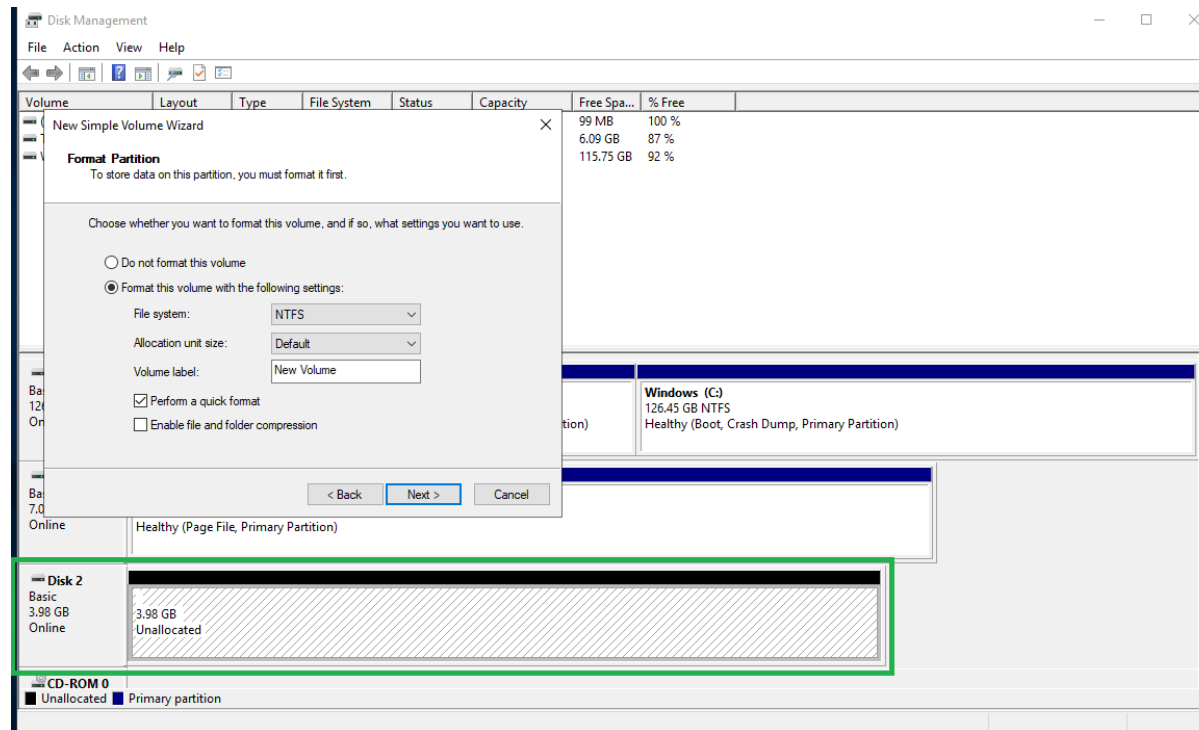
 Create and attach a new disk  Attach existing disks

LUN ⓘ	Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...)	Encryption
0 ▾	Disk2Files ✓	Standard SSD (l... ▾	4	120	25	Platform-

Зайдіть на віртуальну машину - доданий диск має статус «Unallocated». Виконайте «New simple Volume» – визначте літеру, і відформатуйте диск (рис. 1). Перевірте, що новий диск додано до ВМ.



File and Storage Services->Volumes-> Disks



На ВМ – відключить IE Enhanced Security Configuration, використовуйте Server Manager/Local Server (рис. 2).

Server Manager

Server Manager ▶ Local Server

ManageToolsViewHelp

Dashboard

Local Server

All Servers

File and Storage Services ▶

PROPERTIES

For VM1

TASKS

Computer name	VM1	Last installed updates	Today at 1:19 PM
Workgroup	WORKGROUP	Windows Update	Install updates automatically using Windows Update
		Last checked for updates	Today at 1:12 PM
Windows Defender Firewall	Public: On	Windows Defender Antivirus	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	Off
NIC Teaming	Disabled	Time zone	(UTC) Coordinated Universal Time
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00430-00000-00000-AA471 (activated)
Operating system version	Microsoft Windows Server 2019 Datacenter	Processors	Intel(R) Xeon(R) Platinum 8171M CPU @ 2.1 GHz
Hardware information	Microsoft Corporation Virtual Machine	Installed memory (RAM)	4 GB
		Total disk space	138.51 GB

Питання

1. Що таке snapshot у SMB File Share і які типові сценарії його використання?
2. Які механізми використовуються для створення snapshot'ів у Windows Server та Azure Files?
3. Чим відрізняються snapshots від повноцінних резервних копій?
4. Як працює доступ до попередніх версій файлів (Previous Versions) у SMB-шерінгу?
5. Які переваги підходу “Lift and Shift” під час міграції файлових серверів у хмару?
6. У яких випадках Lift and Shift-міграція не рекомендується і чому?
7. Які обмеження існують у Azure File Share для SMB-протоколу?
8. Як Python SDK дозволяє працювати з Azure File Share: створення файлів, папок і snapshot'ів?
9. Які відмінності між File Share та Blob Storage в Azure для сценаріїв з SMB?
10. Як відбувається синхронізація серверів за допомогою Azure File Sync Agent?
11. Що таке Cloud Tiering у Azure File Sync і як воно працює?
12. Як забезпечується консистентність даних між локальним сервером і Azure File Share?
13. Які метрики важливо моніторити у File Sync-інфраструктурі (latency, sync status, journal size тощо)?
14. Як масштабувати файлове сховище у Azure File Share при зростанні обсягу даних або навантаження?
15. Які типові проблеми можуть виникнути під час синхронізації через Azure File Sync та як їх діагностувати?