CONFIGURING & MANAGING DATA STORAGE ON WINDOWS SERVER 2019

CHI GEORGE MOFOR

Provisioning

Optimization

Security

Table of Contents

TABLE OF FIGURES

CONFIGURING AND MANAGING DATA STORAGE ON WINDOWS SERVER 2019

1. INTRODUCTION

Data is at the heart of every IT infrastructure. Configuring and managing data storage properly on Windows Server 2019 ensures availability, integrity, and performance for enterprise applications. Windows Server 2019 offers multiple storage management tools and technologies for both traditional and software-defined environments.

Data storage is a fundamental role of Windows Server 2019. By installing the File and Storage Services role, a server can act as a central file server where users store and share data. File and Storage Services "includes technologies that help you set up and manage one or more file servers, which are servers that provide central locations on your network where you can store files and share them with users". In a lab environment, I implemented storage by adding disks, creating partitions and volumes, and configuring shares and quotas. Windows Server 2019 provides features like NTFS (New Technology File System) and ReFS (Resilient File System) file systems, Storage Spaces for virtual pools, FSRM (File Server Resource Manager) for quotas, and BitLocker for encryption. This report covers these concepts and how to implement them in a server lab, including practical step-by-step procedures.

2. DISK TYPES & FILE SYSTEMS

Windows Server supports different disk and volume types. Basic disks use standard MBR or GPT partition tables and hold simple volumes (partitions). In contrast, Dynamic disks allow software-based RAID (spanned, striped, mirrored, RAID-5 volumes) across multiple disks. However, note that dynamic disks are deprecated in modern Windows (except for boot-volume mirroring); Microsoft recommends using Storage Spaces instead for resilience. When initializing a disk, you choose MBR (Master Boot Record) or GPT (GUID Partition Table) partition style. MBR is limited to ~2 TB per partition, whereas GPT can support vastly larger disks (theoretical limits in zettabytes). For example, any disk or volume above 2 TB must use GPT; otherwise, Windows cannot address the extra space. Windows Server 2019 also supports legacy FAT32 and exFAT formats (for small USB drives, etc.), but the two primary file systems are NTFS and ReFS. NTFS is the default, providing features like ACL security descriptors, encryption, disk quotas, and rich metadata. Beginning with Server 2019, the Resilient File System (ReFS) offers even greater scalability and data integrity features. In practice, NTFS is used for most server volumes; ReFS is typically used on Storage Spaces for virtualization or archive storage.
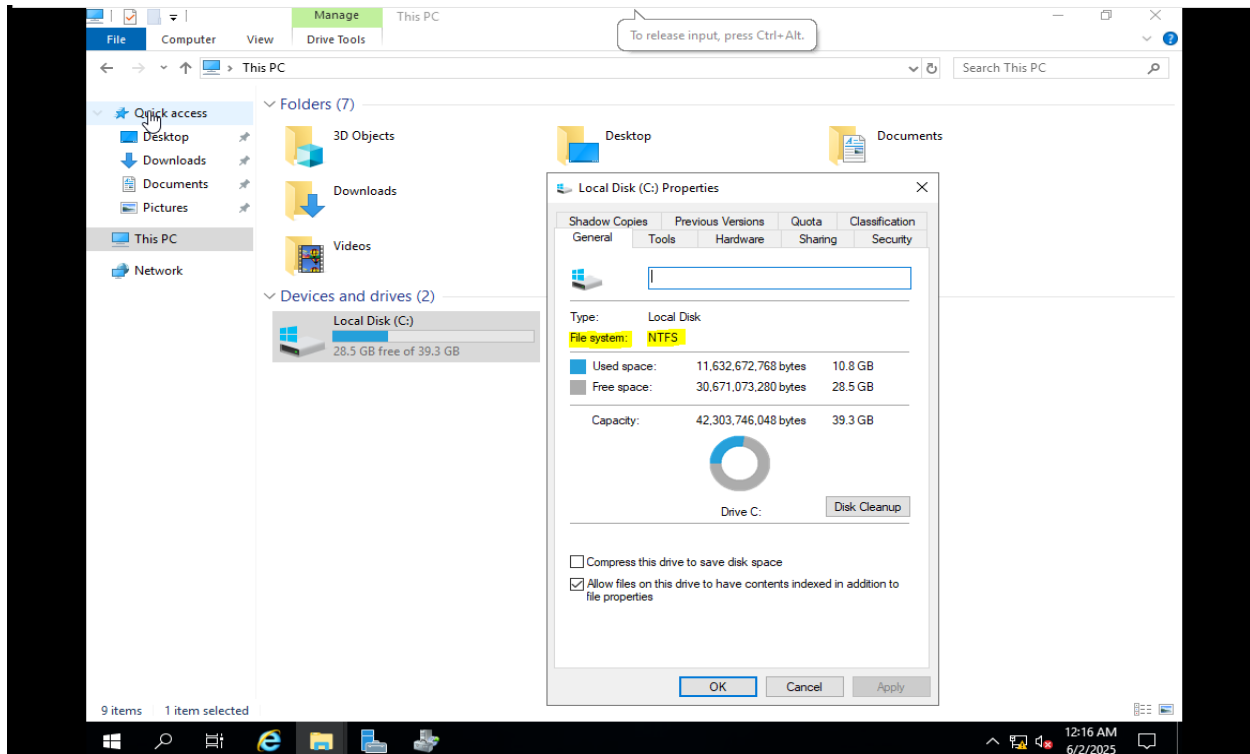

Figure 1: Windows Server2019 with NTFS

3. ADDING AND INITIALIZING DISKS

Adding and initializing disks is a fundamental task in managing data storage on a Windows Server. Whether deploying a new server, expanding existing storage, or preparing a virtualization environment, administrators must often add new physical or virtual disks and prepare them for use.

Before any data can be stored on a new disk, it must first be detected by the operating system, brought online, and initialized. **Initialization** is the process of configuring the disk with a **partition style** — either **MBR (Master Boot Record)** or **GPT (GUID Partition Table)** — which allows the server to understand how to organize data on the disk.

This process is applicable in several scenarios:

- Setting up a **new Windows Server** with unformatted disks.

- **Expanding storage capacity** by adding new drives to a server or virtual machine.

- Reconfiguring drives for use in **RAID arrays, Storage Spaces, or ReFS volumes**.

- Creating **dedicated storage volumes** for specific services such as Hyper-V, file servers, or backup systems.

Using the **Disk Management utility** or **PowerShell**, administrators can initialize, partition, and format these new disks according to storage requirements and best practices. The choice between MBR and GPT depends on the size and use case of the disk:

- **MBR** supports up to 2 TB and 4 primary partitions.

- **GPT** supports disks larger than 2 TB and is recommended for most modern deployments.

The following section walks through the lab steps for adding and initializing disks in **Windows Server 2019**, using both **GUI** (Disk Management) and **PowerShell** approaches.

3.1 Steps to add and initialize a disk in windows server 2019 (VMware) using Disk Management Utility.

Part 1: Add a Virtual Disk in VMware

1. Shut down your Windows Server 2019 VM (optional but recommended).

2. In VMware Workstation:

   - Right-click the VM > Settings or Edit virtual machine settings.

   - Click Add... > Hard Disk.

   - Choose NVMe (default), then click Next.

   - Select Create a new virtual disk.

   - Set disk size (e.g., 10 GB or more).

   - Choose Store as a single file and click Finish.

3. Start your VM.

Part 2: Initialize the New Disk in Windows Server

Option A: Using Disk Management (GUI)

1. Log in to Windows Server 2019.

2. Open Server Manager > Tools > Computer Management.

3. Go to Disk Management.

4. A pop-up may appear prompting for disk initialization.

   - Choose GPT (recommended for modern systems).
   - Click OK.

If the pop-up doesn't appear:

   - Locate the new disk marked as Unknown / Not Initialized.

   - Right-click on the disk label (e.g., "Disk 1") > Initialize Disk.

- Select GPT and click OK.

5. Right-click on the Unallocated space > New Simple Volume.

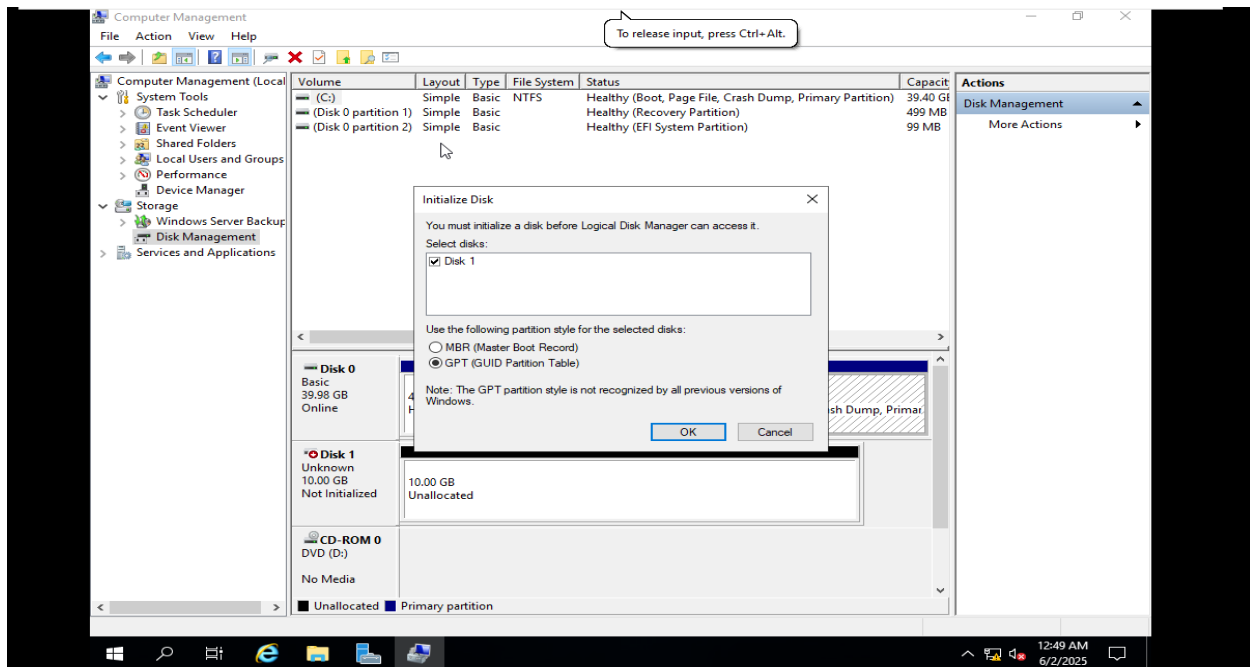- Follow the wizard: assign drive letter, file system (NTFS), and format.
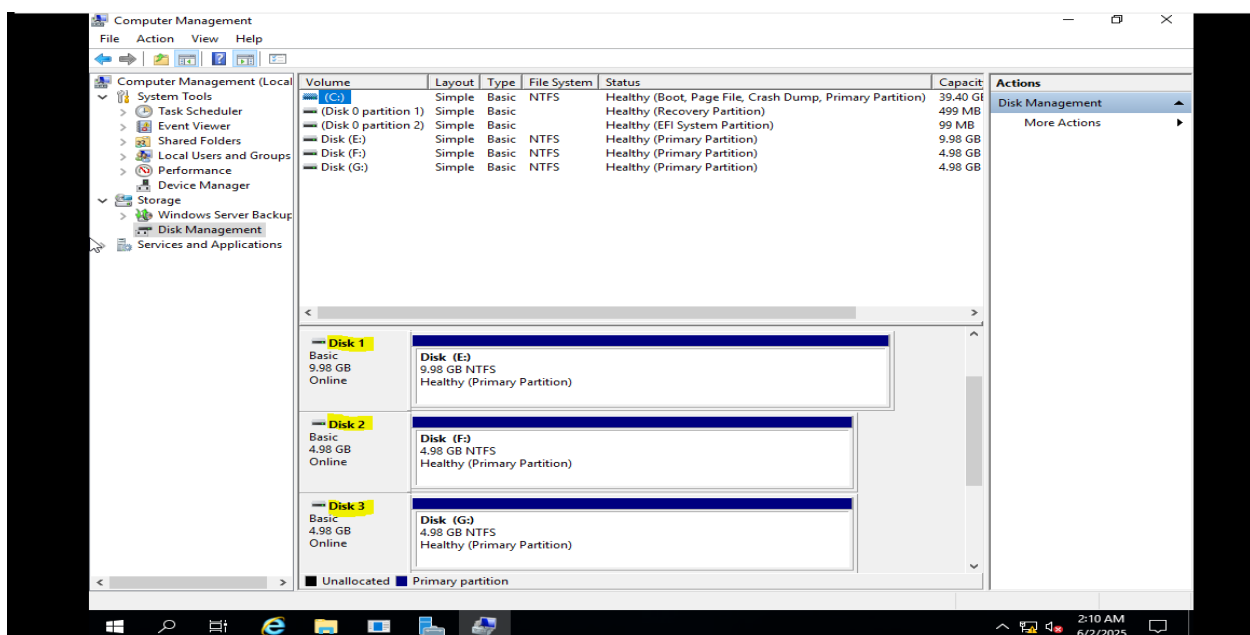

Figure 2: Initializing Disk

Figure 3:Disk Management utility in Windows Server 2019, showing multiple drives and partitions

4. STORAGE SPACES & STORAGE POOLS

Storage Spaces and Storage Pools are advanced storage management technologies built into Windows Server 2019. They provide an efficient, flexible, and fault-tolerant way of managing disk storage. Instead of managing each physical disk separately, administrators can pool them into one logical unit and create virtual disks with features such as mirroring, striping, and parity for redundancy and performance.

This technology is particularly useful in enterprise environments and virtual labs where high availability and storage scalability are critical.

4.1 What is a Storage Pool?

A **Storage Pool** is a collection of physical disks grouped together to create a flexible storage foundation. These disks can be internal, external, or virtual (e.g., VHDX in virtual labs). Once grouped, these disks behave as one pool of capacity.

4.2 What is a Storage Space?

A Storage Space is a virtual disk created from a storage pool in Windows. It allows administrators to combine multiple physical disks into one or more virtual drives that provide improved performance, redundancy, or both, depending on the selected resiliency type.

The resiliency type determines how data is stored and protected across the physical disks.

- **Simple (striped)** – Mainly for performance and has no redundancy. Data is **striped** across multiple disks, which improves read/write performance. However, if any disk fails, all data is lost.

- **Mirror (two-way or three-way)** – Used for redundancy and high availability. Data is written to **two or more disks**, so if one or even two disks fail (in a three-way mirror), the data remains accessible.

- **Parity** – Purposefully for space-efficient redundancy. Data and parity (recovery) information are distributed across all disks. In case of a single disk failure, data can be reconstructed from the parity.

This abstraction allows you to manage storage intelligently and flexibly while providing fault tolerance.

4.3 Setting Storage Pool and Storage Spaces

1. Open Server Manager

   - Server Manager→ File and Storage Services → Storage Pools

2. Create a Storage Pool

   - Click Tasks → New Storage Pool

   - Name the pool (e.g., *Group1 StoragePooling*)

   - Select available physical disks (e.g., 3 x 10 GB virtual disks)

   - Confirm and complete the wizard.
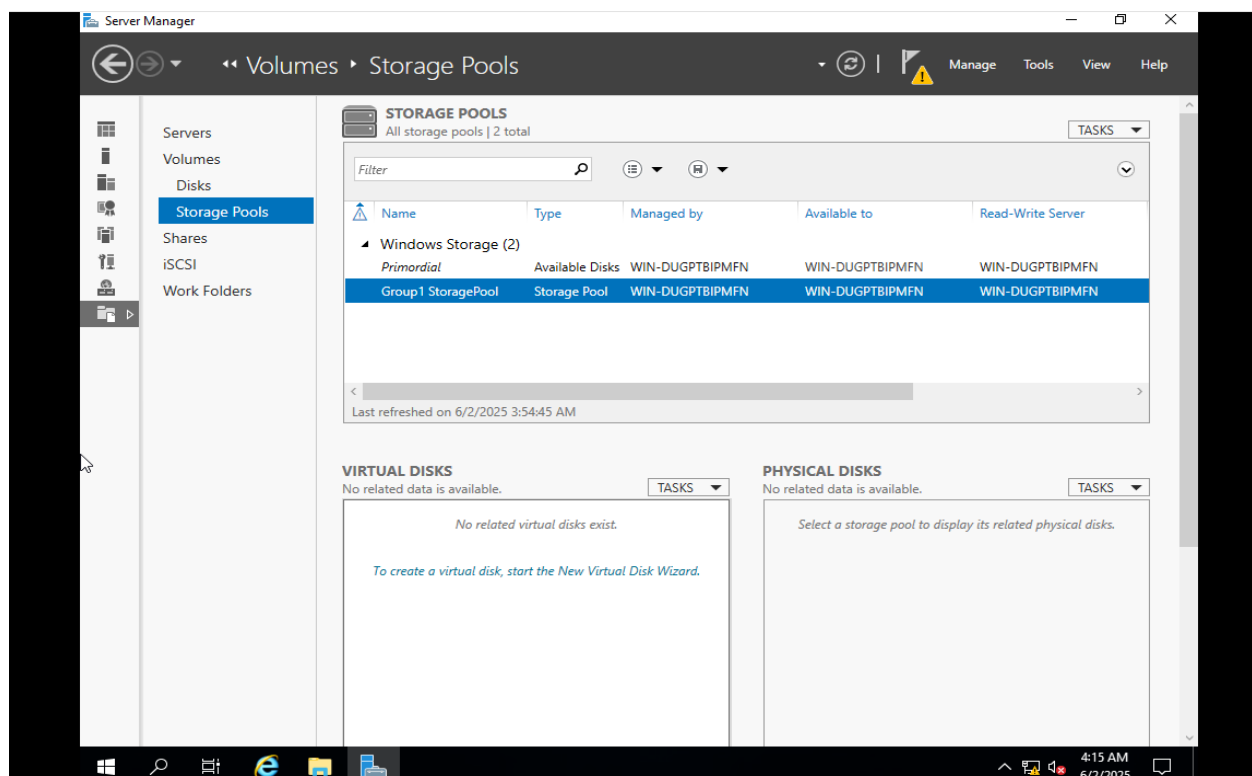
Figure 4: Server Manager "Storage Pools" view. We have created a storage pool named "Group1 StoragePool" from one physical disk

3. Create a Virtual Disk (Storage Space)

- After creating the pool, click Tasks → New Virtual Disk

- Choose the Storage Pool created

- Name the disk (e.g. *Virtual Disk*)

- Select Resiliency Type (e.g., Two-way Mirror)

- Set size (e.g., 10 GB)

- Finish the wizard.

Figure 5: Creation of the virtual Disk. Encountered errors, since WinServer was able to read just one disk for the storage pool and virtual Disk required more than one storage

4. Create a Volume

- After creating the virtual disk, you will be prompted to create a volume

- Assign a drive letter
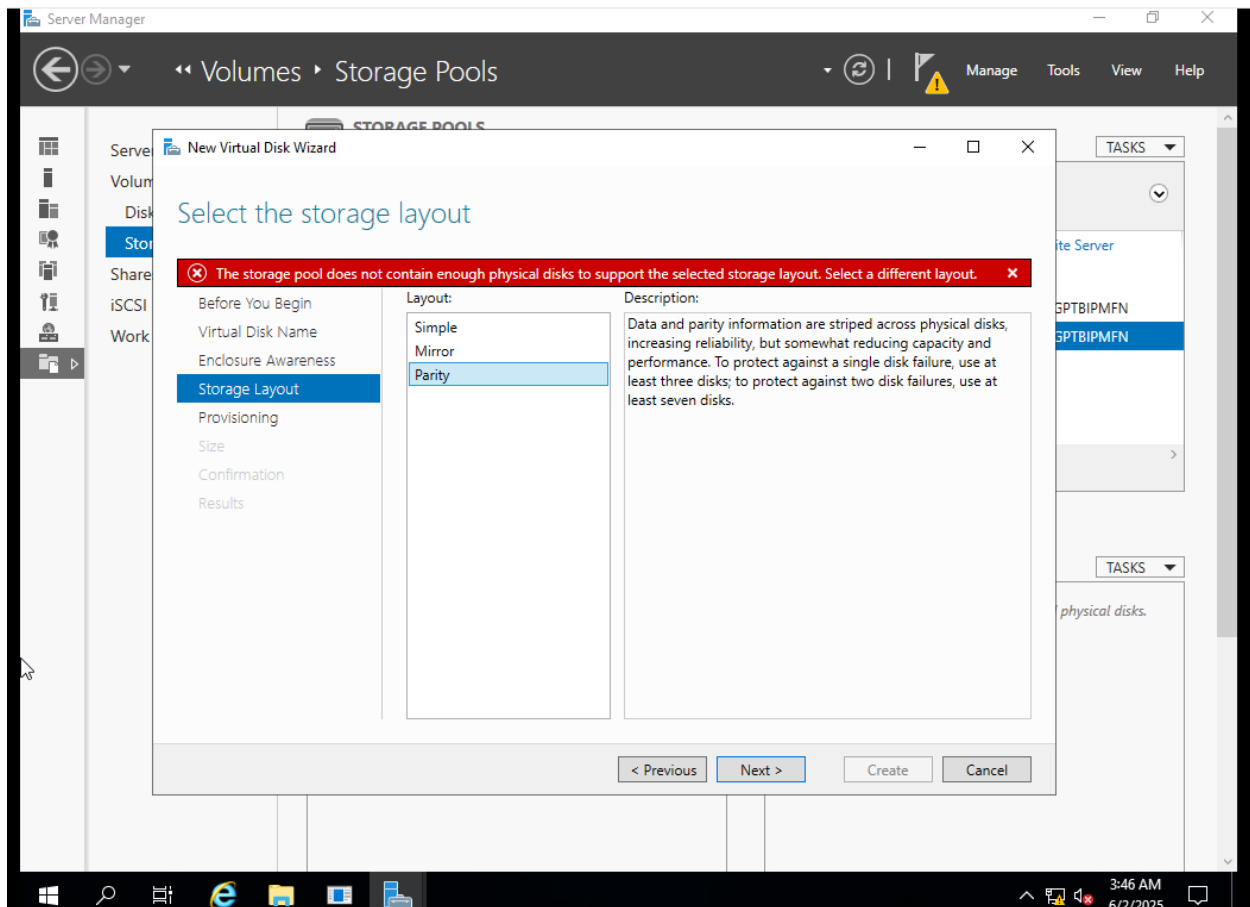
- Format the volume (usually NTFS)

- Finish the wizard. The volume appears under This PC in Windows Explorer.

4.4 Benefits of Storage Spaces and Storage Pools

- **High Availability**: Mirror and parity spaces ensure data remains accessible even if a disk fails.

- **Flexibility**: Easily extend storage by adding more disks to the pool.

- **Cost Efficiency**: Use commodity hardware instead of expensive RAID systems.

- **Tiered Storage**: Mix SSDs and HDDs for performance and capacity optimization.

- **Replacement for Dynamic Disks**: Microsoft recommends Storage Spaces instead of legacy dynamic disks.

5. FILE SERVER QUOTAS (FSRM)

File Server Quotas are an essential feature used to manage and control disk space usage on Windows servers. They help prevent individual users or departments from consuming excessive storage, which could impact the overall performance and availability of file server resources.

5.1 Definition and Purpose

The **File Server Resource Manager (FSRM)** is a role in Windows Server that provides a set of tools for managing and monitoring storage on file servers. One of its core features is **quota management**, which allows administrators to limit the amount of space that can be used on a folder or volume. Quotas can be used to enforce organizational storage policies, prevent runaway storage usage, and ensure fair resource allocation.

5.2 Creating Quotas on Windows Server

To implement quotas, we first installed the File Server Resource Manager role using Server Manager. Once installed, we accessed the FSRM tool by navigating to: Tools → File Server Resource Manager.

Under the Quota Management section, we created a new quota on a specific folder — for example, applying a 200 GB hard quota to the E:\ShareDocs folder. FSRM allows administrators to use pre-defined quota templates or create custom ones depending on the storage requirements.

There are two main types of quotas:

- **Hard Quota**: Prevents users from saving additional data once the limit is reached.

- **Soft Quota**: Does not block usage but sends notifications when thresholds are exceeded.

We also saw how to configured **email notifications** to alert administrators when usage exceeds certain thresholds, such as 85%. To test this, we temporarily set a soft quota to **100MB** and uploaded files beyond the limit to trigger the alert.

5.3 Storage Resource Management Service (SRMSVC)

This is the **service behind FSRM (File Server Resource Manager)**, which is used to manage:

- Quotas (limit space usage on folders/volumes)

- File screening (block certain file types)
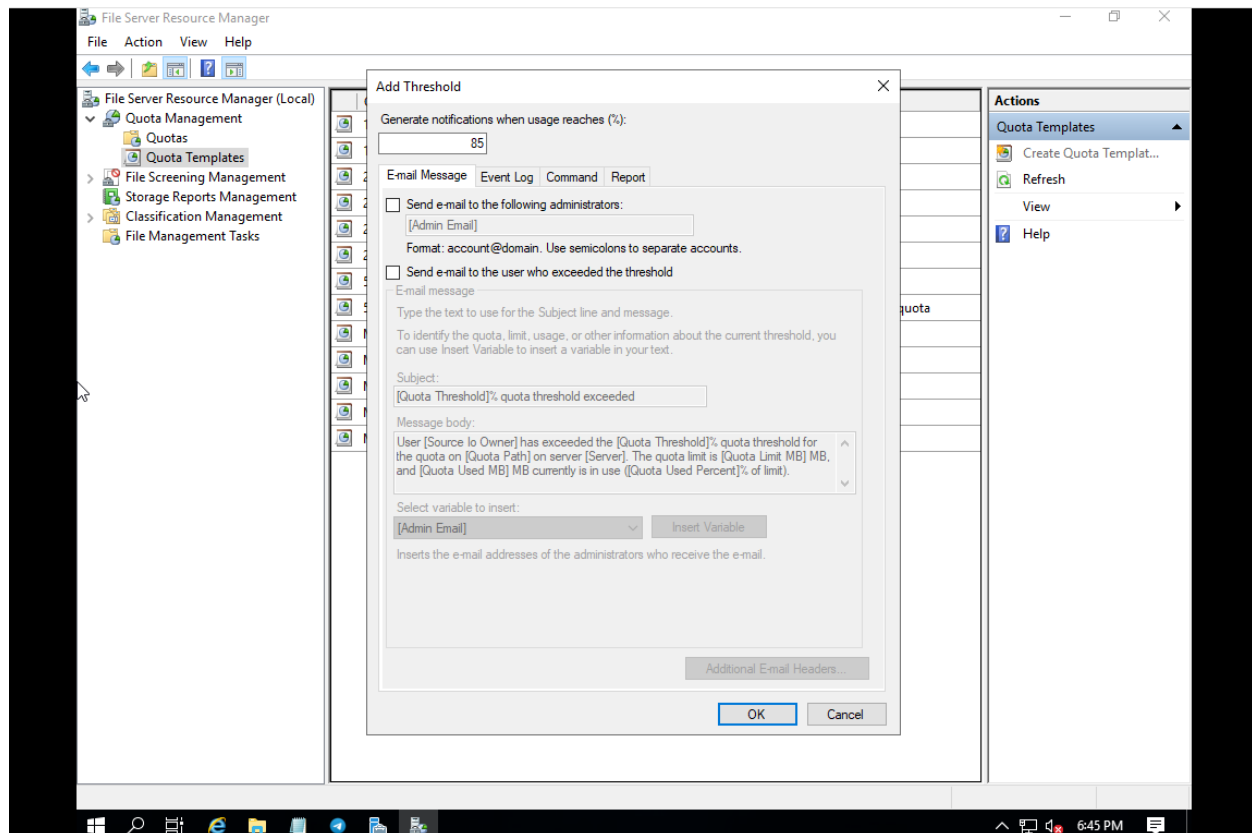
- Storage reports

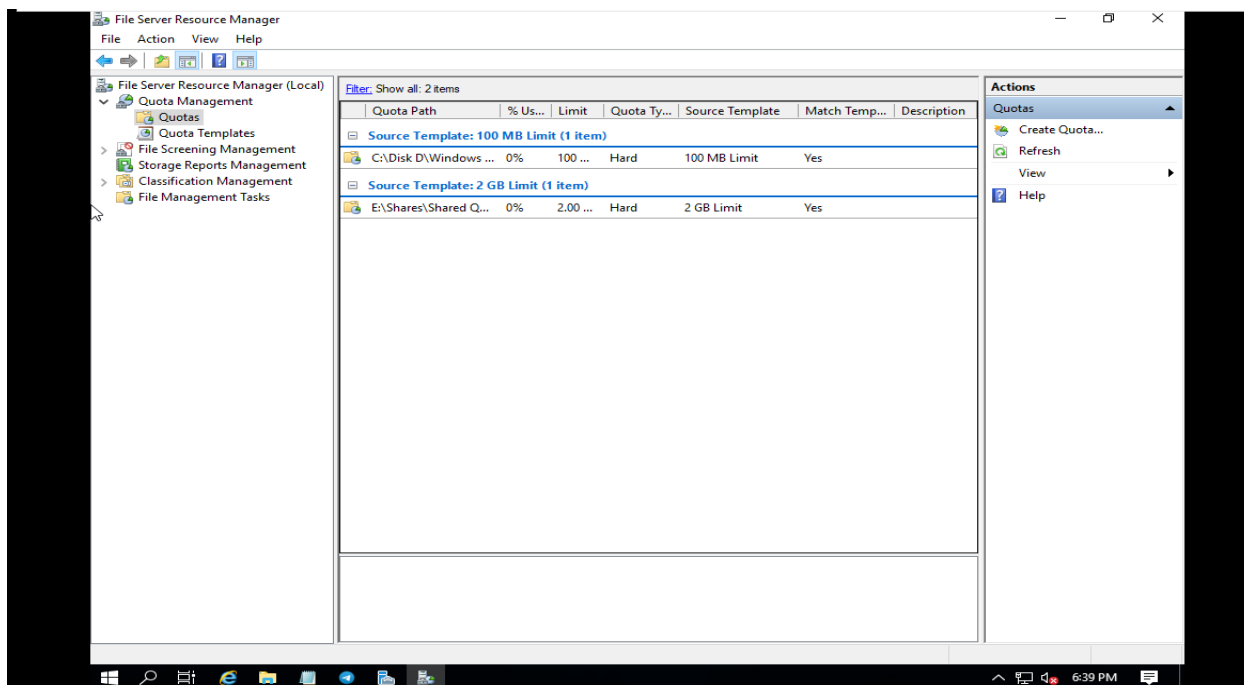*Figure 6: Creating a quota template of 85% thresholds*
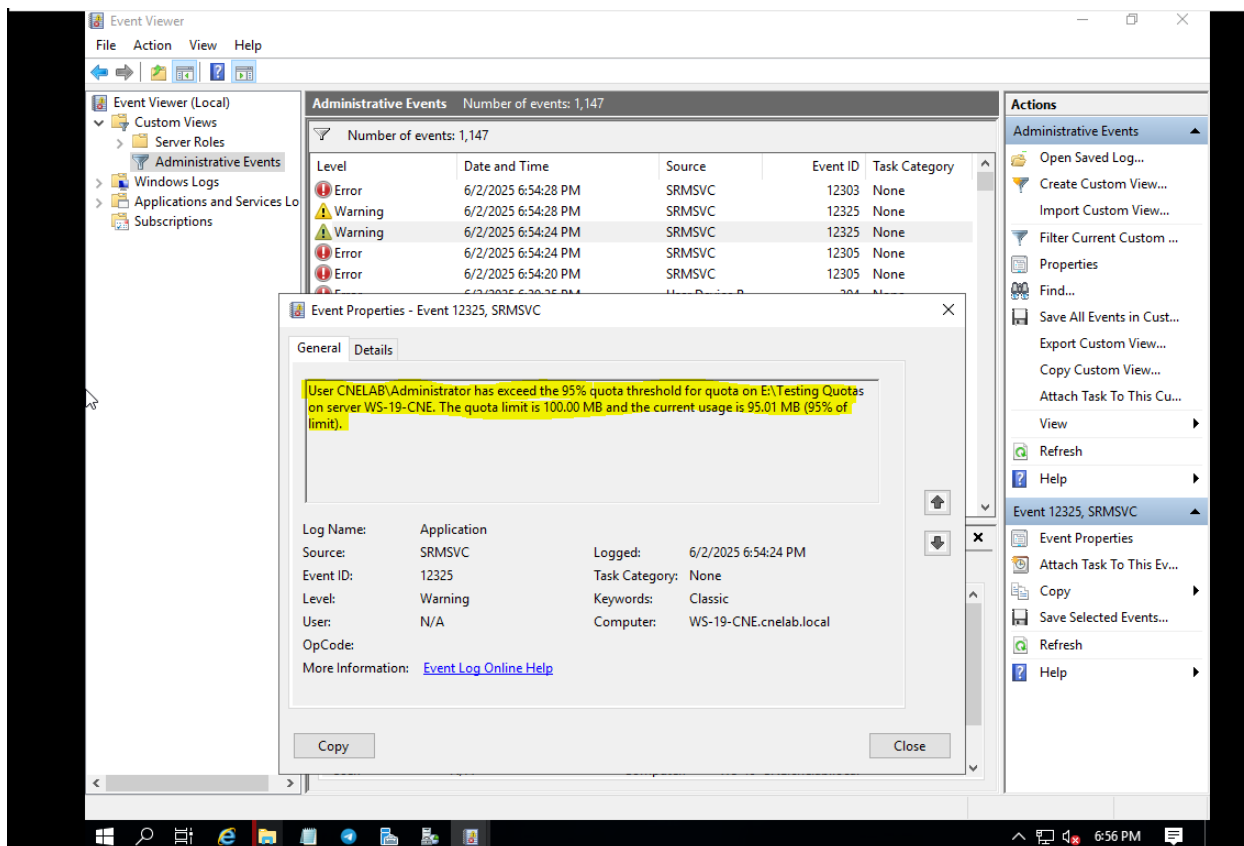
Figure 7: Quotas created

Figure 8: User Admin has exceeded the 95% quota threshold

5.4 Advantages of FSRM Quotas

- **Granular control**: Quotas can be applied per-folder, not just per volume.

- **Custom notifications**: Administrators can receive alerts before limits are fully reached.

- **Templates and automation**: Use of pre-defined templates makes quota deployment faster.

- **Better than NTFS quotas**: FSRM offers more flexibility and detailed reporting than traditional NTFS disk quota tools.

- **Additional features**: FSRM also supports disk usage reporting and file screening to block unwanted file types, although this lab focused only on quota management.

6. BITLOCKER DRIVE ENCRYPTION

BitLocker Drive Encryption is a built-in security feature in Windows Server and Windows operating systems that provides full volume encryption to protect data at rest. It is designed to prevent unauthorized access to data on lost or stolen drives by encrypting the entire disk. BitLocker is especially effective when combined with hardware-based protection like the Trusted Platform Module (TPM).

The primary purpose of BitLocker is to safeguard sensitive data stored on a server or workstation, particularly in environments where physical security cannot be guaranteed. For example, if a server hard drive is removed and connected to another system, the data will remain inaccessible without proper authentication.

6.1 Steps On Implementing BitLocker

1. Install the BitLocker Feature

- Open Server Manager

- Go to Manage → Add Roles and Features

- Under Features, select BitLocker Drive Encryption

- Complete the installation and restart if necessary

2. Enable BitLocker on a Drive

- Open File Explorer

- Right-click the desired volume (e.g., D:, E:) and select Turn on BitLocker

- Choose to use the TPM only or TPM + PIN for added security at boot

- Select where to save the recovery key (e.g., USB, file, or print)

- Choose encryption type (e.g., XTS-AES 128-bit or 256-bit)

- Start the encryption process and wait for completion

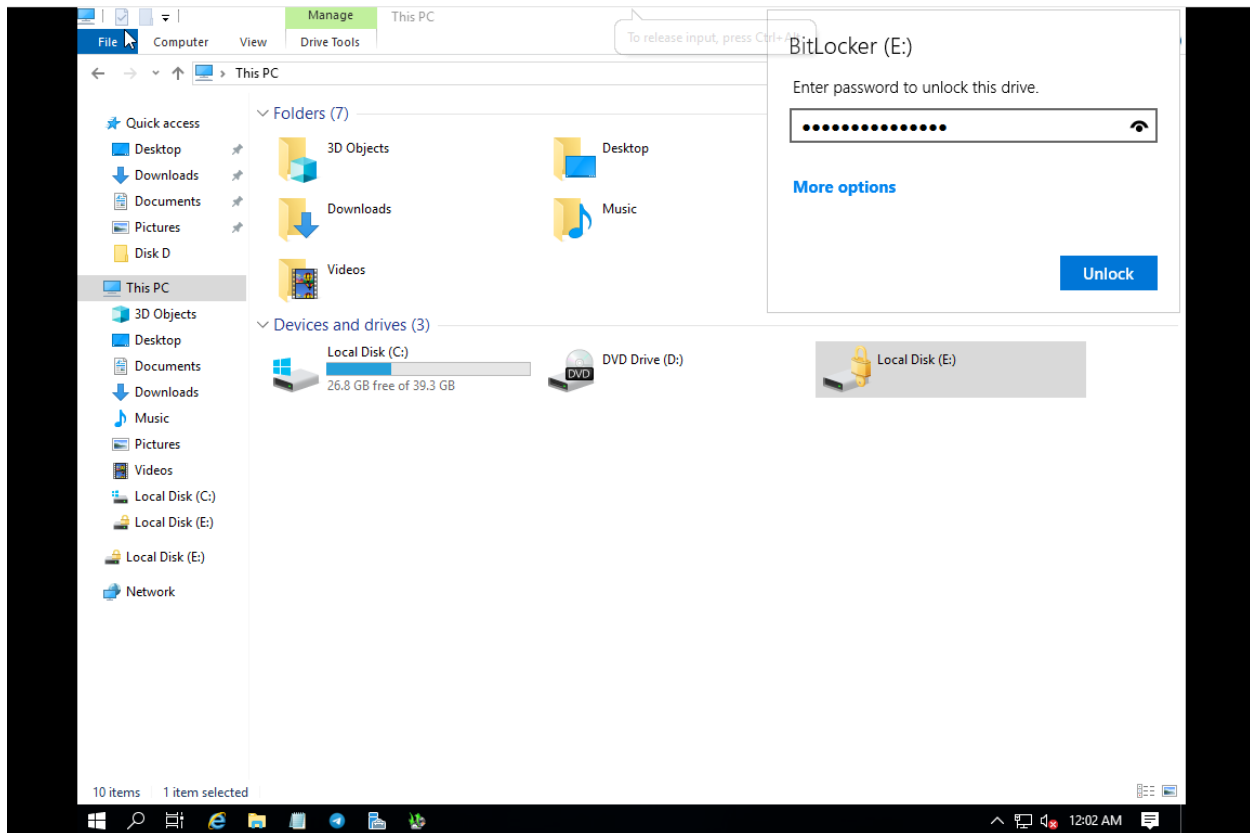- The drive will show a lock icon indicating it is protected

Figure 9:Lock icon showing how Drive is encrypted with BitLocker

6.2 Advantages of BitLocker

- **Full Volume Encryption**: Protects all files including temporary and system files.

- **Data Theft Protection**: Prevents access if a physical drive is stolen or removed.

- **TPM Integration**: Leverages hardware-level security to prevent tampering.

- **Recovery Key Support**: Ensures recovery even if credentials are forgotten.

- **Minimal Performance Impact**: Encryption is optimized and efficient.

- **Works with NTFS, FAT32**: Supports various file systems commonly used on Windows.

7. MONITORING DISK USAGE & HEALTH

Monitoring disk usage and health is a critical aspect of system administration in Windows Server environments. It ensures the early detection of hardware failures, helps track storage capacity trends, and supports optimal performance. Administrators rely on various built-in tools to continuously observe and report the status of both physical and virtual disks.

7.1 Tools & Techniques For Monitoring

1. Performance Monitor (PerfMon)

- Found under *perfmon.msc*

- Tracks disk metrics using counters like:

  - **PhysicalDisk**: I/O latency, disk queue length, throughput

  - **LogicalDisk**: Free space, read/write activity

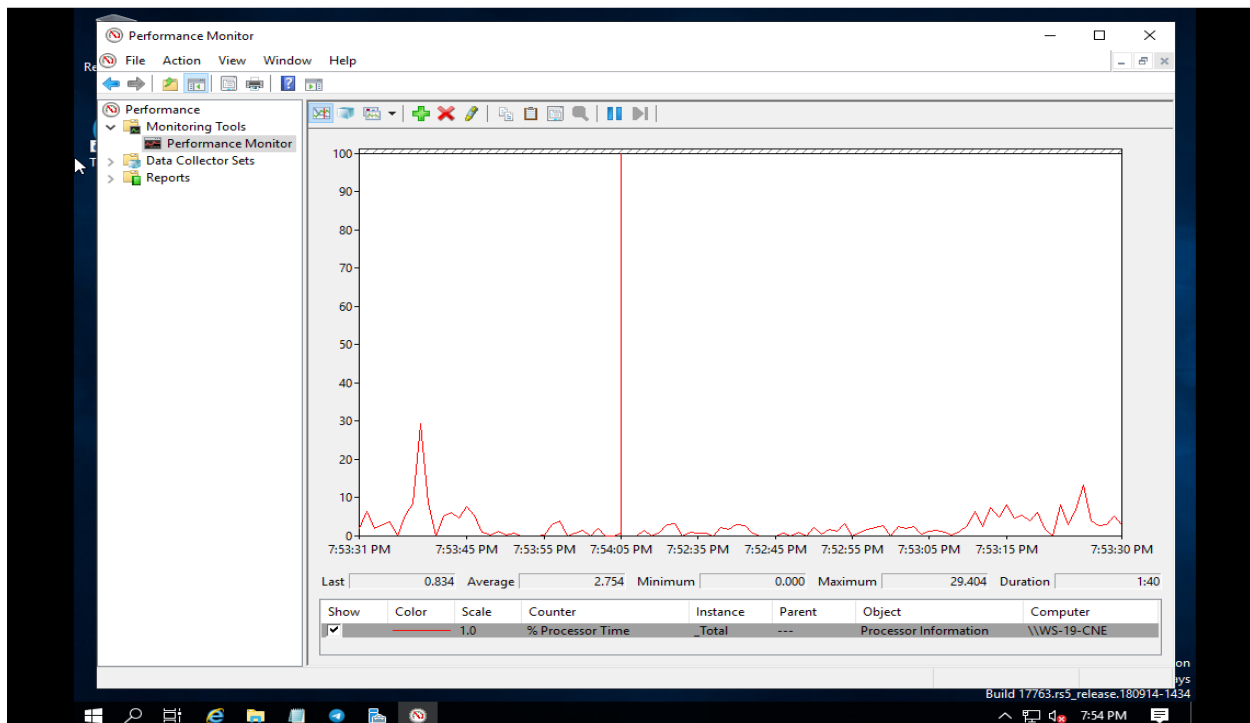- Useful for setting up alerts and performance baselines

Figure 10: Performance Monitor

2. Resource Monitor

- Available through Task Manager or directly via *resmon*

- The **Disk** tab shows real-time per-process I/O activity

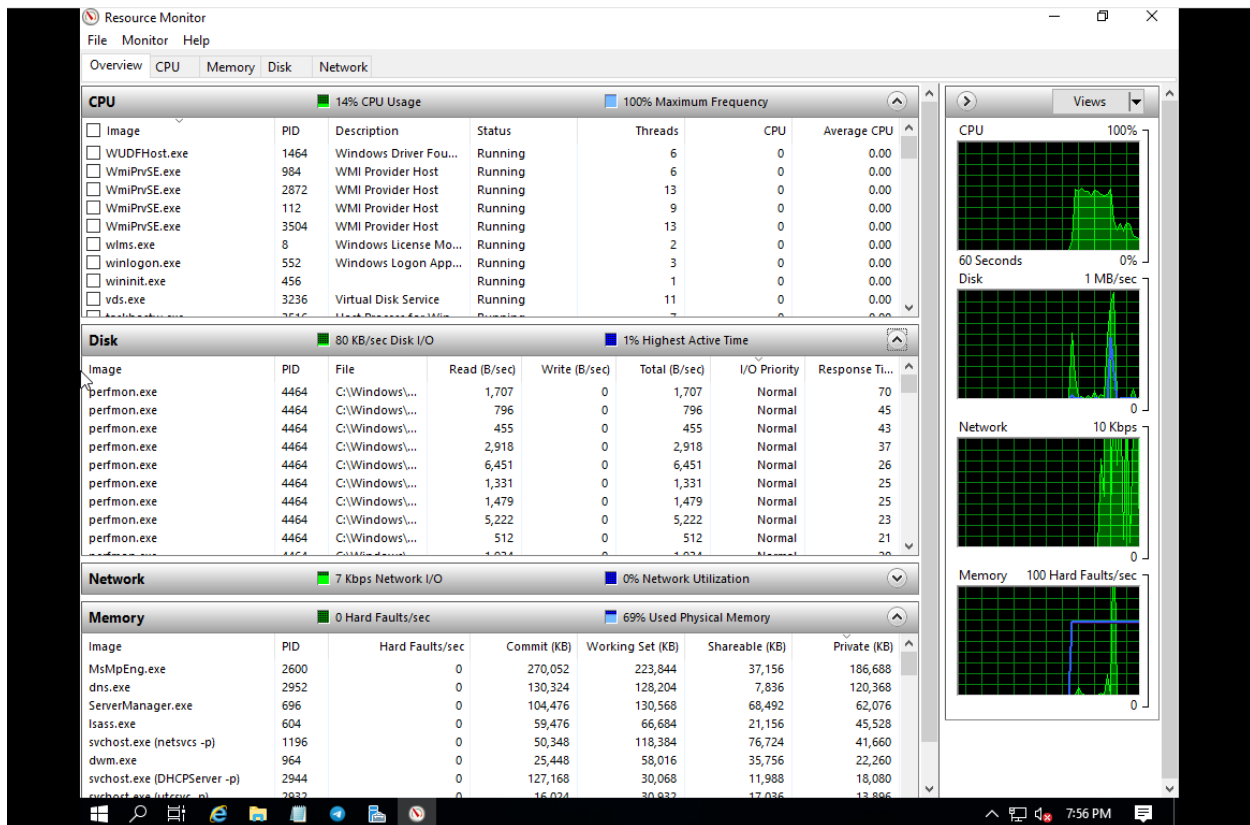- Helps identify which applications are heavily using the disk

Figure 11: Resource Monitoring

3. Event Viewer (S.M.A.R.T. Events)

- Logs critical disk warnings using **Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.)**

- Access via: Event Viewer → Windows Logs → System → Source: Disk

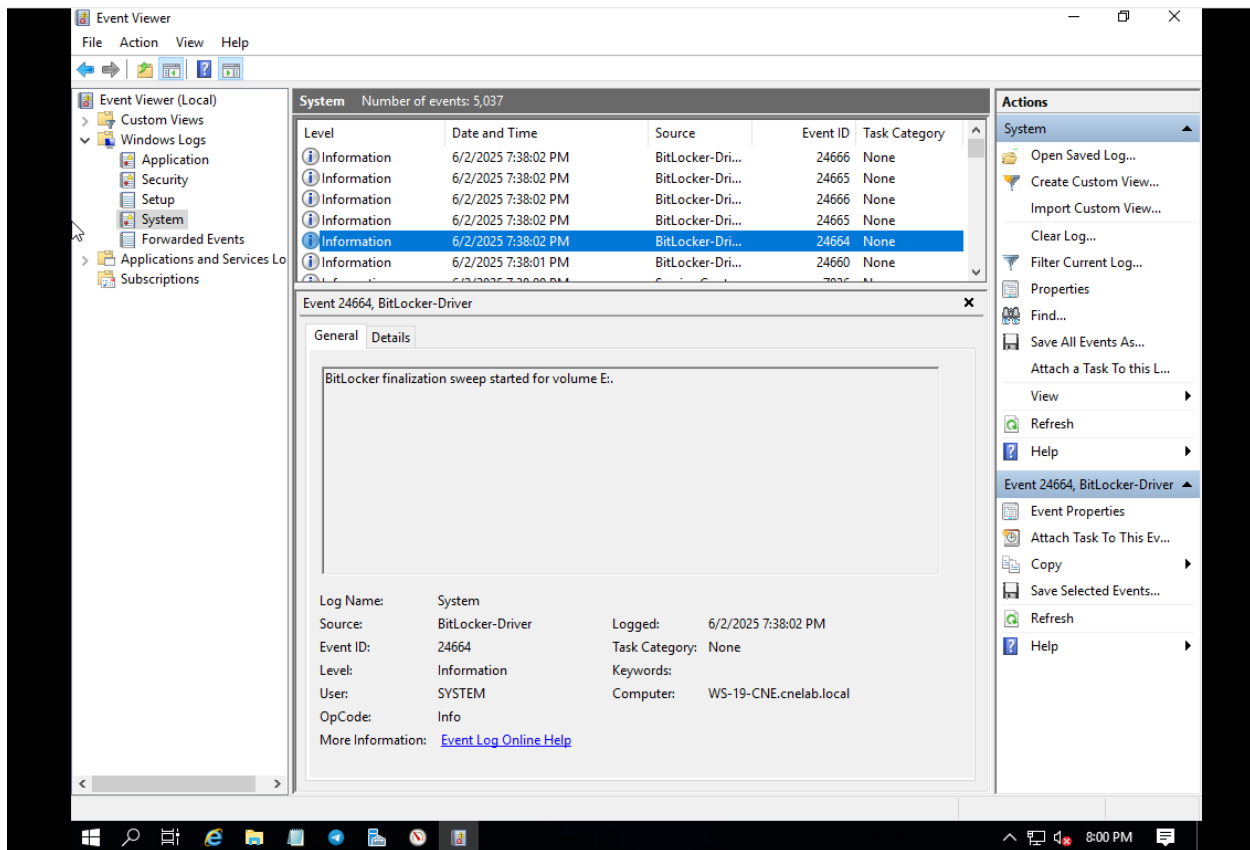- Useful for spotting early signs of disk failure

Figure 12: Event Viewer

4 . PowerShell Disk Health Checks

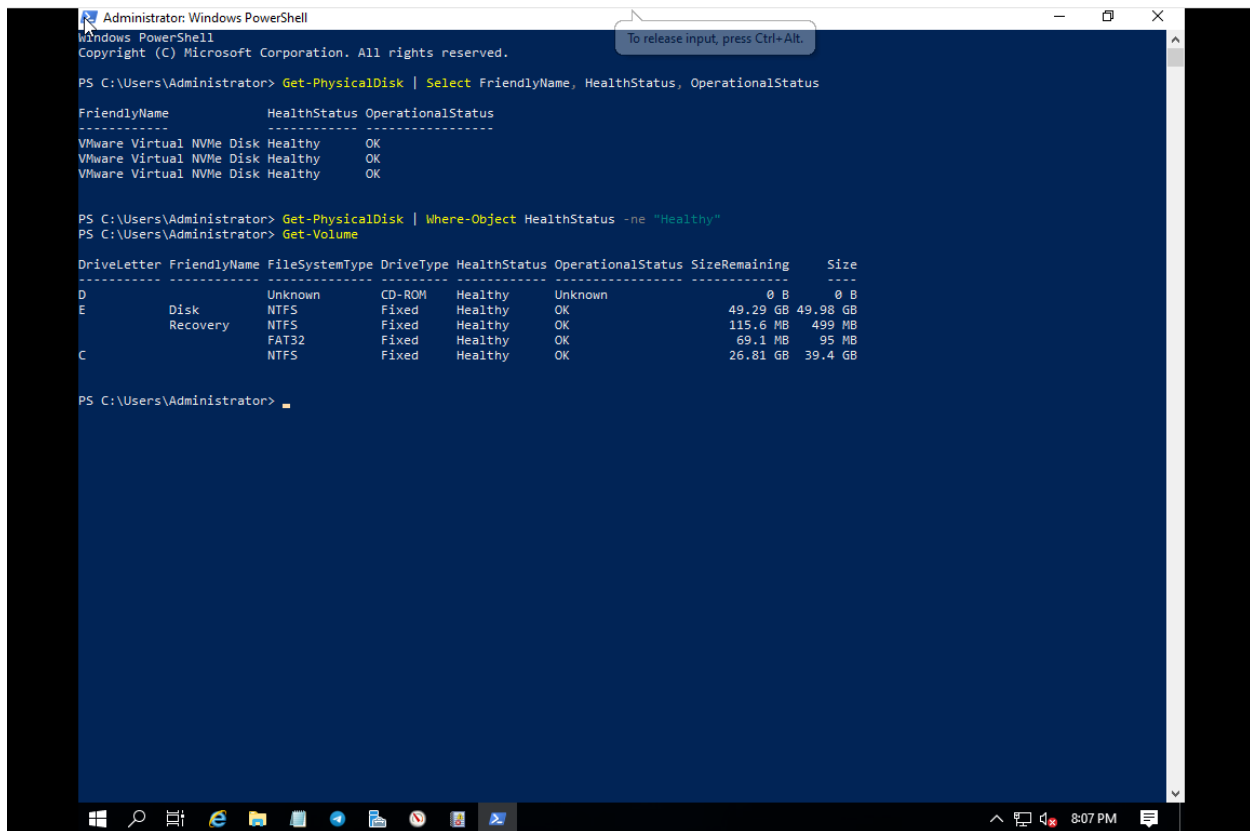- Check the status of physical disks:

Get-PhysicalDisk | Select FriendlyName, HealthStatus, OperationalStatus

- Identify any disk that isn't healthy:

Get-PhysicalDisk | Where-Object HealthStatus -ne "Healthy"

- View volume details such as file system and free space:

Get-Volume

Figure 13: Disks Check With PowerShell

7.2 Advantages of Disk Monitoring

- **Early Warning**: Identifies failing drives before data loss occurs

- **Performance Optimization**: Detects bottlenecks due to disk latency or saturation

- **Capacity Planning**: Monitors space usage trends for future upgrades

- **Data Integrity**: Ensures volumes and pools maintain read/write health

- **Redundancy Checks**: Confirms mirrors and pools function as expected during failure scenarios

8. WINDOWS SERVER BACKUP

Windows Server Backup (WSB) is a built-in feature in Windows Server that provides a simple and effective way to back up and restore server data. It allows administrators to create full or partial backups, including system state, individual volumes, or specific files and folders. WSB is particularly useful for protecting data in small to medium environments or lab setups, where enterprise backup solutions may not be required.

8.1 Purpose and Use

Windows Server Backup is primarily used to:

- Perform full or partial backups of server data

- Create **System State** backups for disaster recovery

- Schedule regular backups to local or external drives

- Restore individual files, folders, or entire volumes

8.2 Implementation Steps

1. **Install the Feature**

   - Go to Server Manager → Add Roles and Features
   - Under Features, select Windows Server Backup, then install

2. **Launch WSB**

   - Open Server Manager → Tools → Windows Server Backup

3. **Choose Backup Type**

   - Click Backup Once… for a one-time backup

   - Or click Backup Schedule… for regular automatic backups

4. **Configure the Backup**

   - In the wizard, select Custom Backup

- Choose the critical volumes to protect (e.g., C: system drive and E: data volume)

- Optionally include System State for recovery of Active Directory and system files

- Choose the destination (e.g., external virtual disk or dedicated backup drive)

5. **Run and Monitor the Backup**

- Launch the backup job and monitor its progress
- Upon completion, check the Backup Status
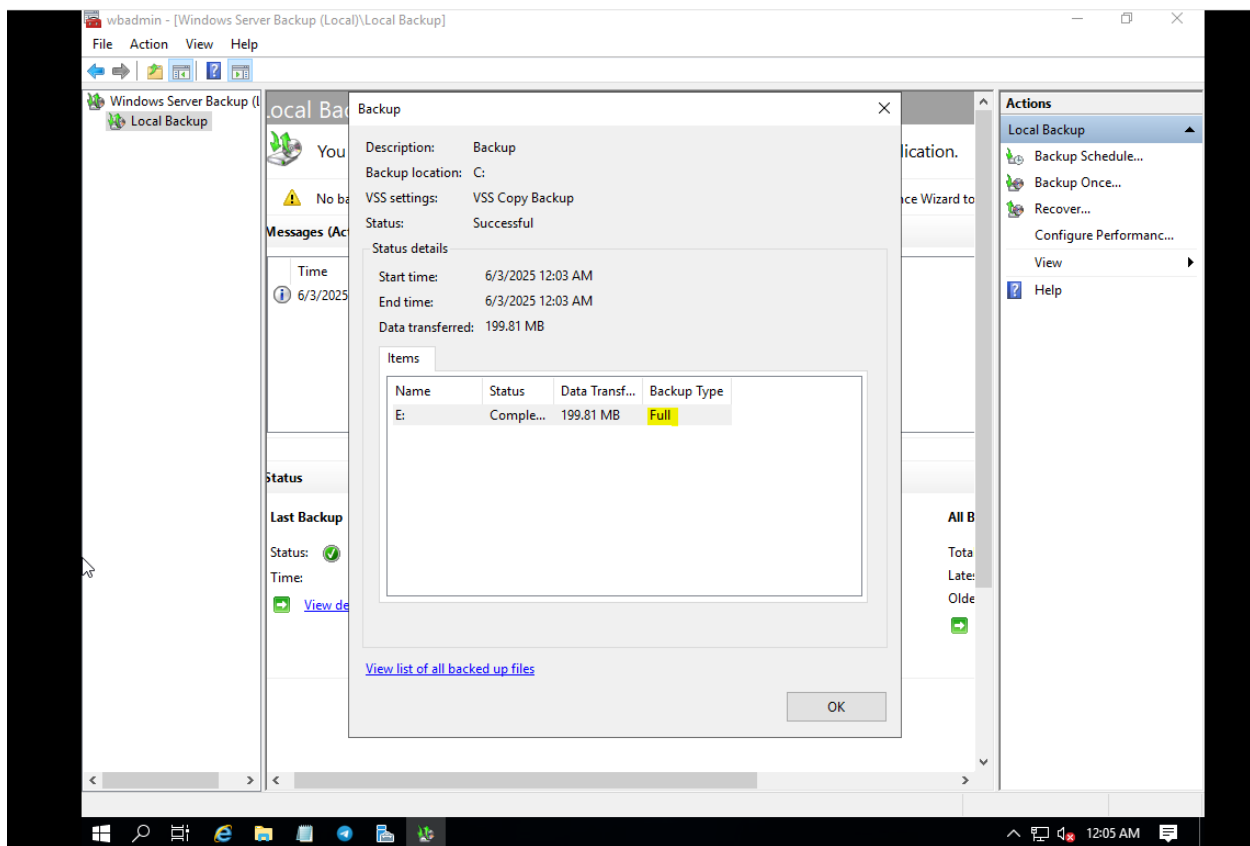- Perform a Recovery Test to verify you can restore files successfully

Figure 14: Complete Full backup of Drive E:

8.3 Available Backup Types in Windows Server

1. **Full Server Backup**

    -   Backs up all volumes, including system files and installed roles

    -   Used for full disaster recovery (bare-metal recovery)

2. **System State Backup**

    -   Includes system files, registry, Active Directory, boot files, and more

    -   Essential for domain controllers and restoring AD environments

3. **Custom Backup**

    -   Allows selection of specific volumes, files, or folders

    -   Useful for backing up critical data without full volume

4. **Incremental Backup (Default Mode)**

    -   Only backs up changes since the last backup

    -   Saves time and storage space

8.4 Advantages of Windows Server Backup

-   **Free & Built-in**: No additional software needed

-   **System State Protection**: Enables domain and configuration recovery

-   **User-Friendly GUI**: Easy to navigate and configure

-   **Flexible Storage**: Supports external disks, DVDs, or network shares (with configuration)

-   **Reliable Recovery**: File-level, volume-level, or full-server restore options

-   **Scheduled Backups**: Automates protection with minimal admin effort

CONCLUSION

This lab offered a comprehensive, hands-on experience in configuring and managing storage within a Windows Server 2019 environment. Through practical, I explored essential tools and technologies that are pivotal for effective storage administration.

Beginning with the differentiation between basic and dynamic disks, I delved into the characteristics of file systems like NTFS and ReFS. Utilizing both Disk Management and PowerShell, I performed tasks such as disk initialization (MBR/GPT), partition creation, volume formatting, and drive letter assignment.

To enhance storage resilience and flexibility, I implemented Storage Spaces by creating storage pools and virtual disks that support redundancy. I configured shared folders with appropriate NTFS and share permissions and applied storage quotas using the File Server Resource Manager (FSRM) to monitor and control disk usage. Data security was addressed by enabling BitLocker encryption on selected volumes, ensuring protection against unauthorized access.

Monitoring the health and performance of storage components was achieved through tools like Performance Monitor, Resource Monitor, and Event Viewer. PowerShell cmdlets were utilized to assess disk health and operational status, with regular checks scheduled to maintain system integrity.

For data protection, Windows Server Backup was deployed to perform full and custom backups, including system state data. The recovery process was tested to confirm the reliability of the backup strategy.

Each configuration step was meticulously documented with screenshots to illustrate procedures and outcomes. Completing this lab has provided a solid foundation in Windows Server 2019's storage capabilities, equipping me with the skills necessary to design, implement, and manage robust storage solutions in real-world scenarios.

GLOSSARY

- **Basic Disk**: A standard disk type using MBR or GPT; supports simple volumes (partitions) on one disk.

- **Dynamic Disk**: A disk type that can contain volumes spanning multiple disks (spanned, striped, mirrored, RAID-5). Deprecated in favor of Storage Spaces.

- **MBR (Master Boot Record)**: Partition style limited to ~2 TB per disk. Requires BIOS to boot.

- **GPT (GUID Partition Table)**: Modern partition style supporting very large disks (up to zettabytes). Required for disks larger than 2 TB.

- **NTFS (New Technology File System)**: Windows file system with support for security ACLs, compression, encryption (BitLocker), quotas, and more.

- **ReFS (Resilient File System)**: Newer Windows file system designed for resilience and scalability; supports integrity streams, large volumes (petabytes), and integrates with Storage Spaces.

- **Volume/Partition**: A formatted storage unit on a disk (e.g., the C: drive). Partitions become volumes once formatted.

- **Drive Letter**: A letter assigned to a volume (e.g., C:, D:) used to access the volume in Windows.

- **Storage Pool**: In Storage Spaces, a collection of physical disks combined into one pool.

- **Virtual Disk (Storage Space)**: A logically created disk within a pool, with selected resiliency options (simple, mirror, parity)..

- **NTFS Permissions (ACLs)**: Security descriptors on files and folders that control user access rights.

- **File Server Resource Manager (FSRM)**: A role service for managing quotas, file screening, and generating storage reports on file servers.

- **Quota**: A storage limit set on a volume or folder; can be hard (enforced) or soft (warning-based).

- **BitLocker**: A full-volume encryption feature in Windows that protects data on drives by requiring a TPM or a recovery key to unlock.

- **Windows Server Backup**: A built-in Windows feature for performing server backups (file-level or bare-metal), with wizard and scheduling support.

- **Disk Management**: A Windows GUI tool (diskmgmt.msc) for performing disk-related tasks like initialization, partitioning, and formatting.

- **Server Manager**: A Windows management console for adding/removing roles and features; includes tools for managing file shares, storage pools, and more.

- **PowerShell**: A command-line shell and scripting environment for Windows administration; storage-related cmdlets include Get-Disk, Initialize-Disk, New-Partition, Format-Volume, Enable-BitLocker, etc.

REFERENCES

1. Microsoft Learn. *File and Storage Services Overview*. Retrieved from: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831487(v=ws.11)

2. Microsoft Learn. *Basic and Dynamic Disks - Win32 apps*. Retrieved from: https://learn.microsoft.com/en-us/windows/win32/fileio/basic-and-dynamic-disks

3. Microsoft Learn. *Windows support for hard disks exceeding 2 TB - Windows Server*. Retrieved from: https://learn.microsoft.com/en-us/troubleshoot/windows-server/backup-and-storage/support-for-hard-disks-exceeding-2-tb

4. Microsoft Learn. *NTFS overview*. Retrieved from: https://learn.microsoft.com/en-us/windows-server/storage/file-server/ntfs-overview

5. YouTube: https://youtube.com/@cbtnuggets?si=O30QEpFH6BDhTTSW