IT 236 Project Report Form

Report Prepared By:	Vivian J. Goshashy
Date:	10/29/2025
Project Phase	Storage and File Management

Section 1: Executive Summary (10 Points)

This phase of the **NewVue Health Infrastructure Modernization Project** focused on expanding storage capacity and implementing a structured, role-based file system on the **NV-FS01** file server. The Proof-of-Concept environment includes **NV-DC1**, which also received an additional data volume for future replication and backup services, and **NV-FS01**, which was configured as the organization's primary file server.

As part of this implementation, several key configurations were completed:

Briefly describe the configurations that were done below

1. **Storage Expansion:** A new 50 GB virtual hard disk was added to both the NV-DC1 (domain controller) and NV-FS01 (file server) virtual machines to provide additional storage capacity.
2. **Disk Preparation:** The new disks on both servers were initialized, formatted, and made ready for data storage within the Windows Server operating system.
3. **Shared Folder Structure:** A logical, department-based folder structure was created on the file server. The main parent folder was then shared across the network, granting "Read" access to all **Authenticated Users**.
4. **Granular NTFS Permissions:** Security was refined using NTFS permissions:

    a. The **root and main departmental folders** were configured with "Read & Execute" permissions, applied to "This folder only," to prevent accidental inheritance of restrictive permissions.
    b. Specific **functional role folders** were granted "Modify" permissions, giving designated users or groups the appropriate level of access for their work.

Collectively, these configurations establish a secure and scalable storage foundation for NewVue Health, ensuring that departmental data is logically organized, protected, and accessible according to role-based permissions across the enterprise.
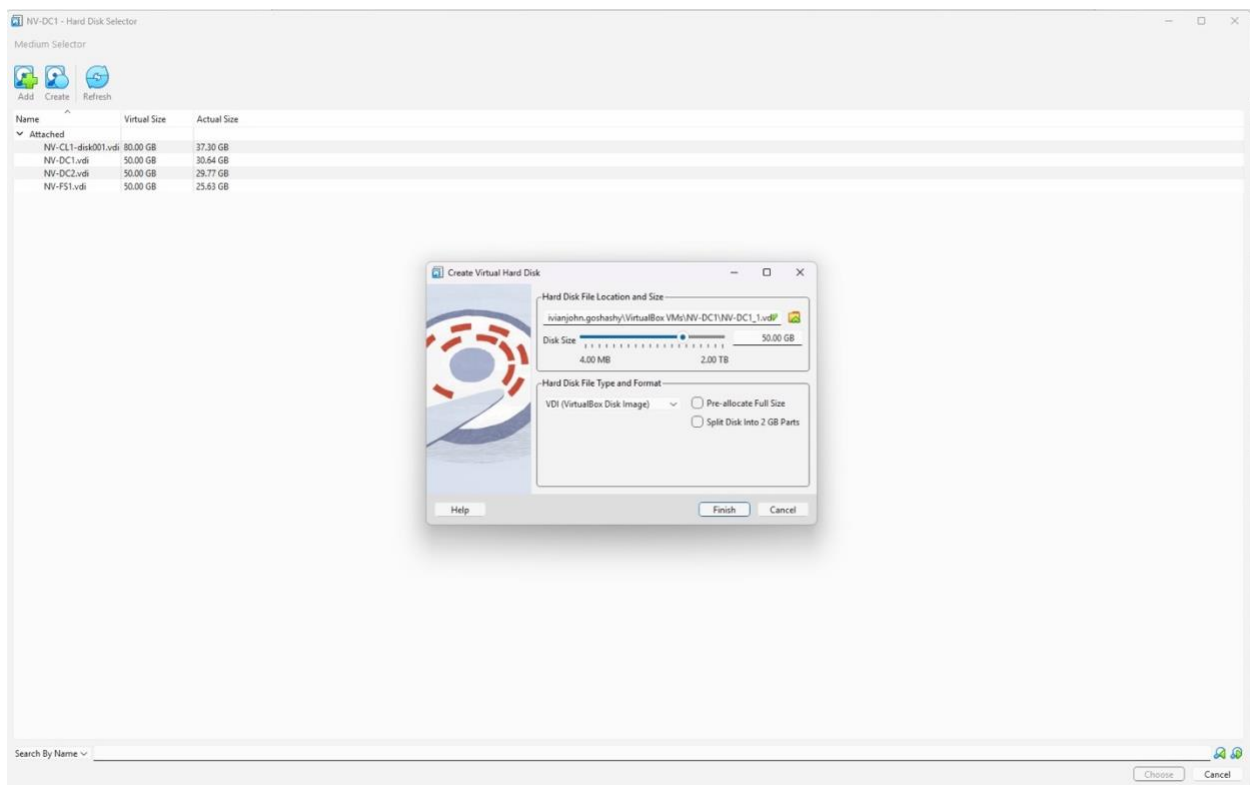
Section 2: Task-Password and Account Lockout Policy (25 points)

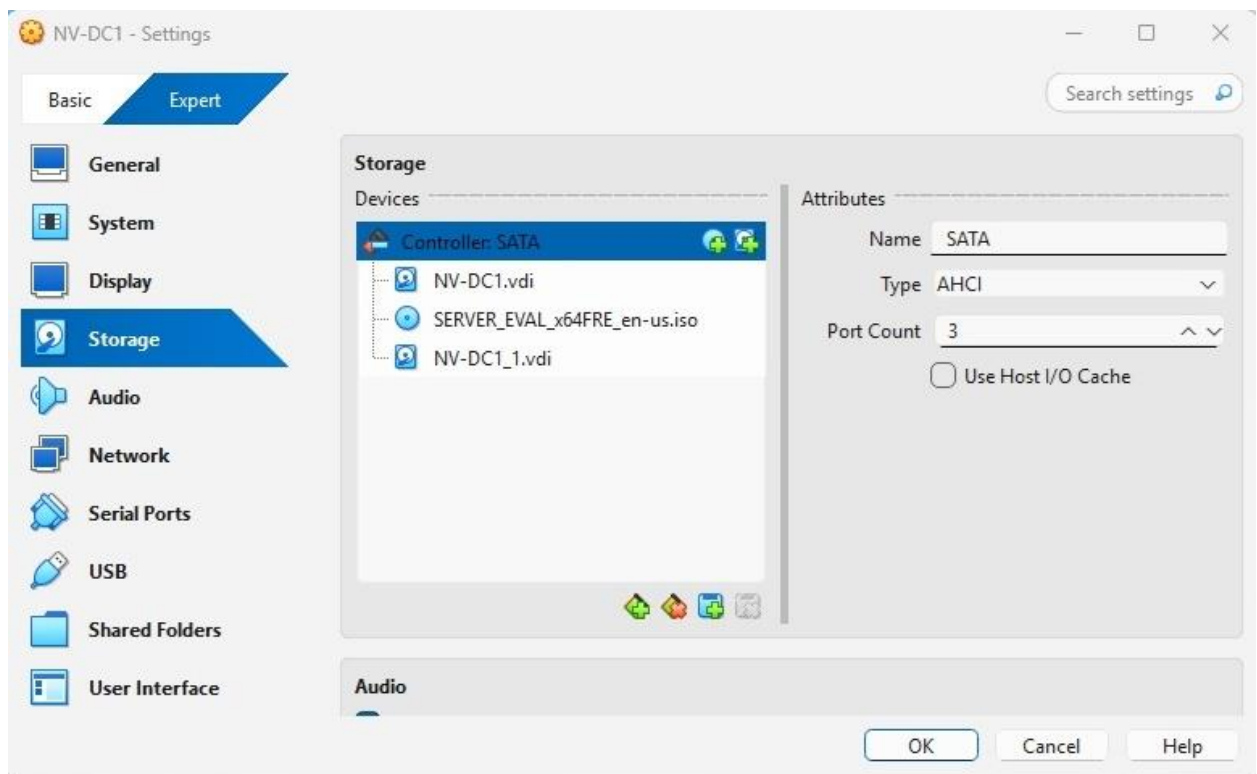### Section 2 – Attaching and Initializing New Storage Drives (20 points)

The new storage disks were created and attached to both **NV-DC1** and **NV-FS01** using Oracle VirtualBox's Storage settings. Each disk was configured as a 50 GB dynamically allocated drive under the SATA controller, then initialized as **GPT** and formatted as **NTFS** within Windows Server.
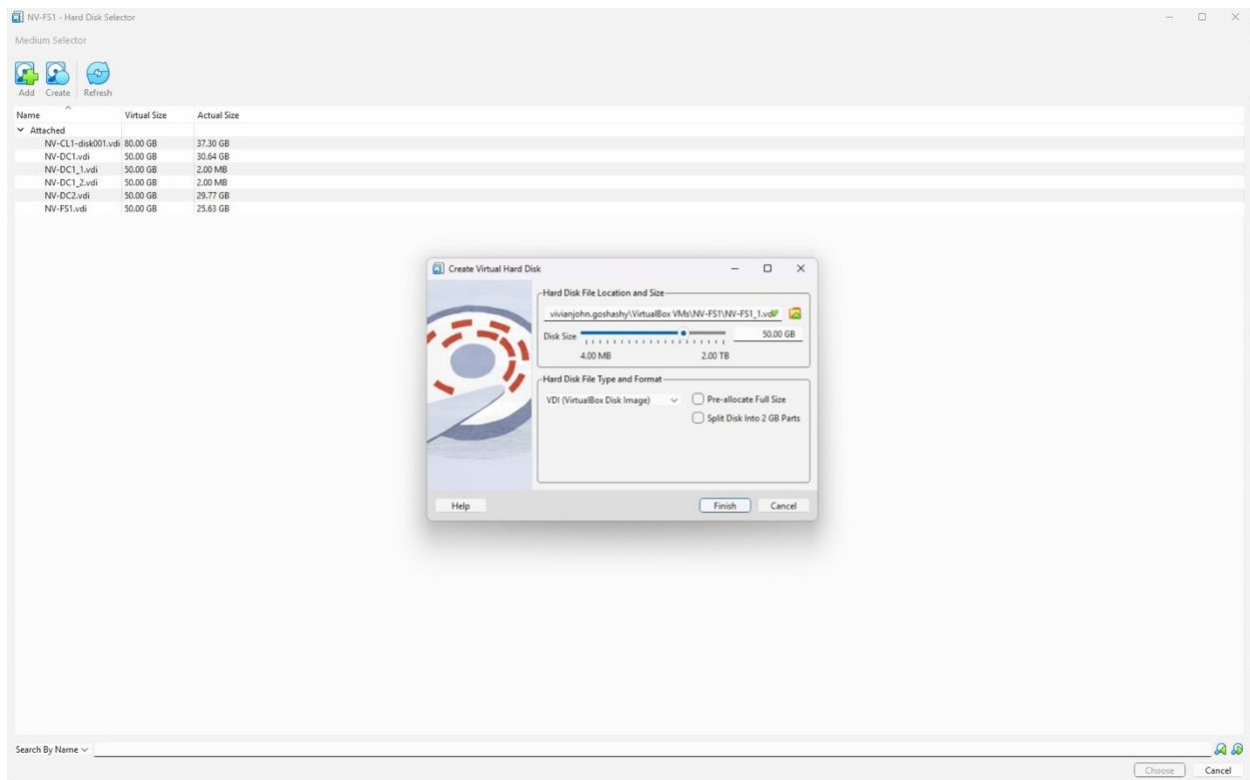
Evidence

- **Evidence 1:** Screenshot of the Create Virtual Hard Disk window (NV-DC1).
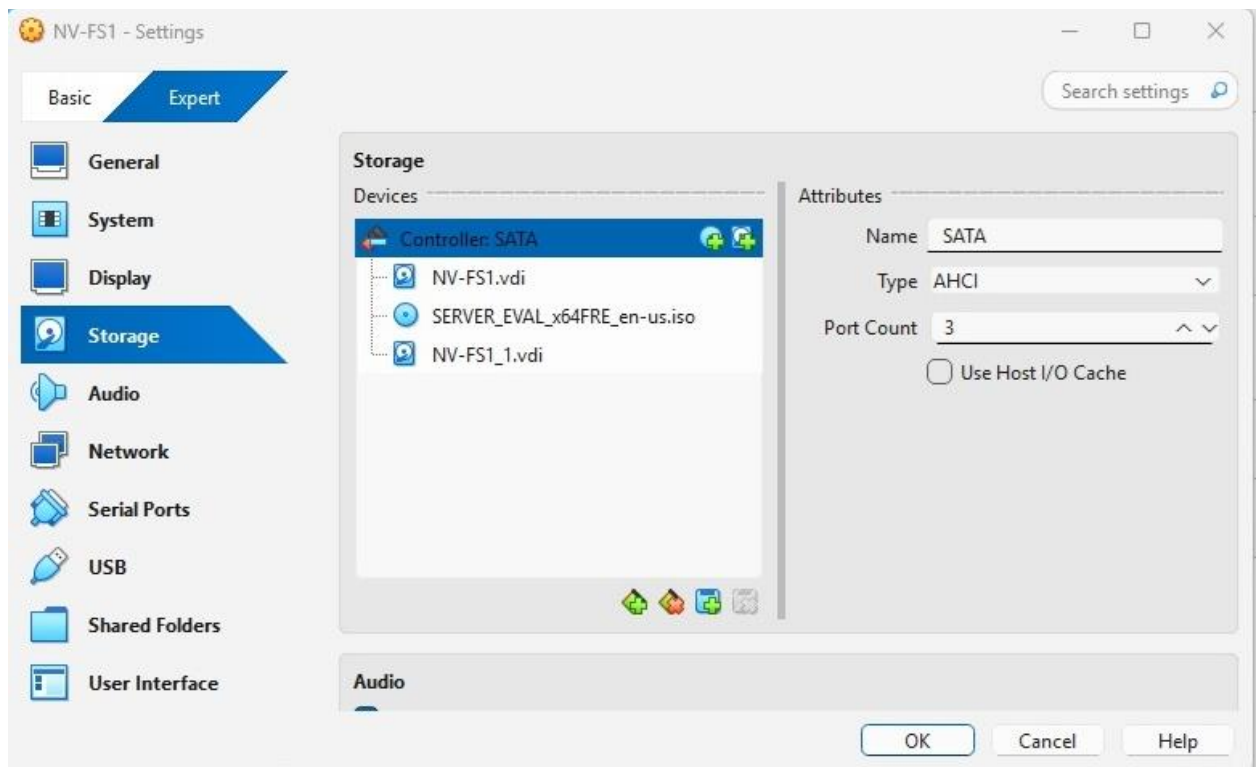
- **Evidence 2:** Screenshot of Storage Settings showing attached disk (NV-DC1).
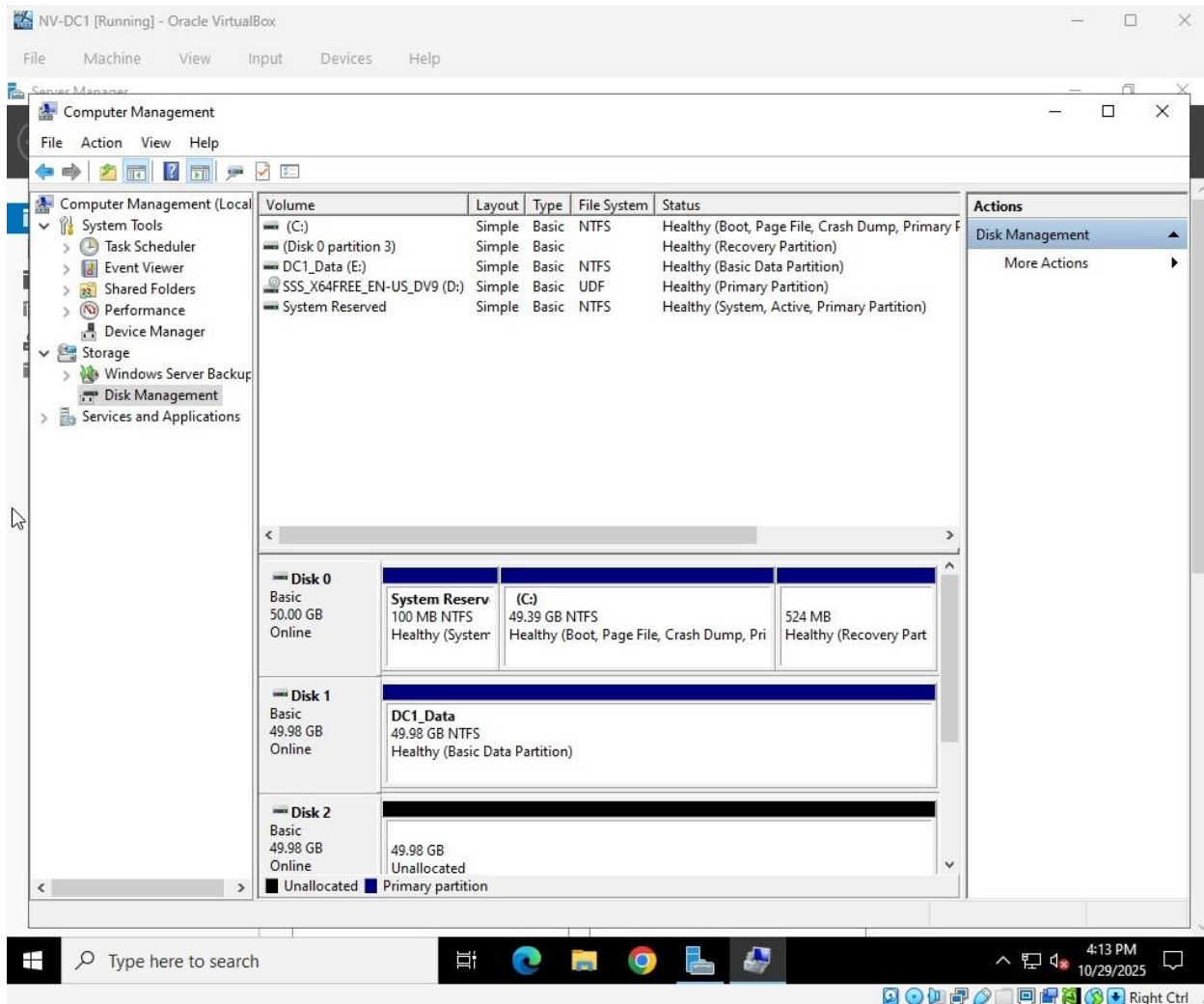
- **Evidence 3:** Screenshot of the Create Virtual Hard Disk window (NV-FS01).
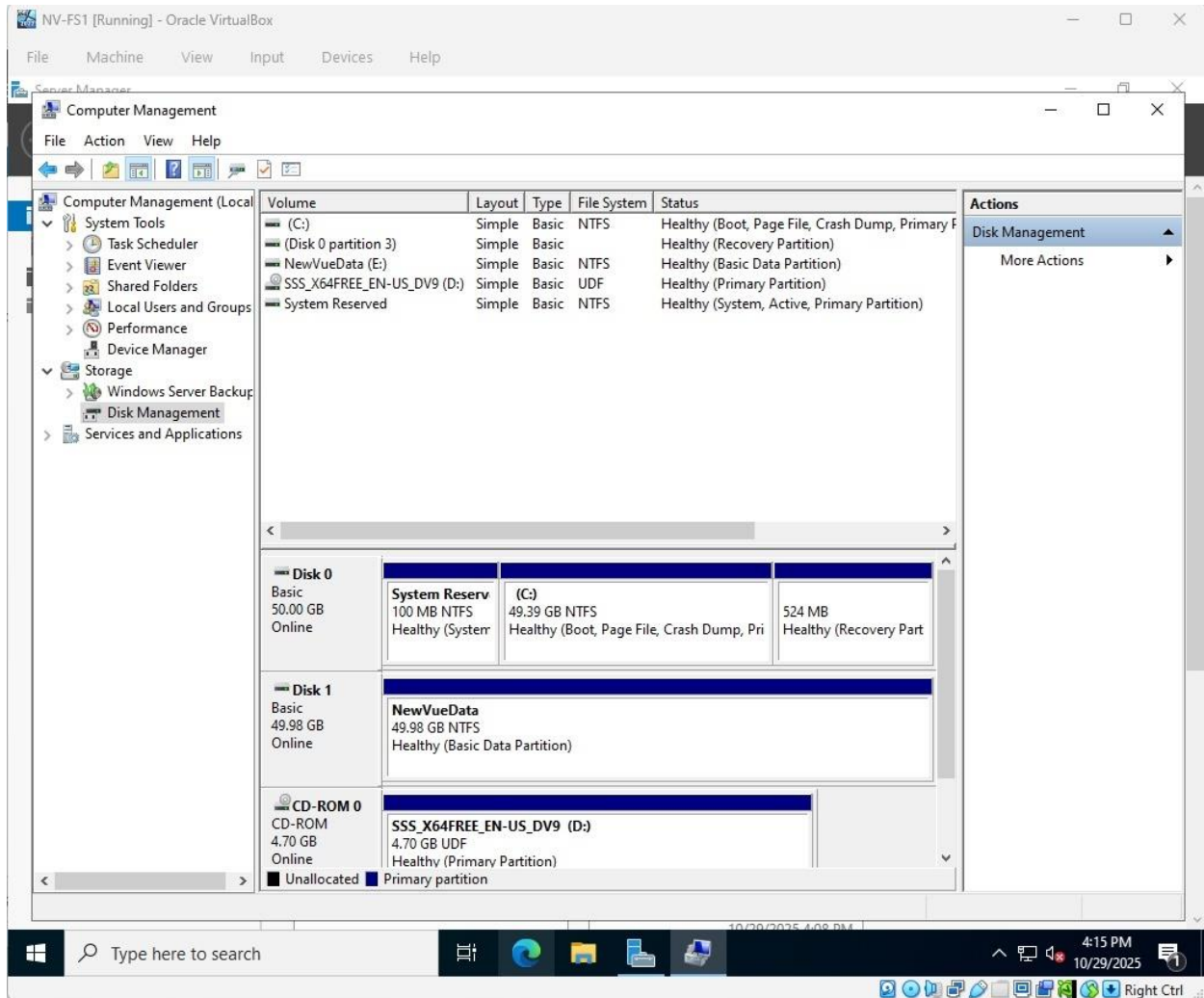

- **Evidence 4:** Screenshot of Storage Settings showing attached disk (NV-FS01).

- **Evidence 5:** Screenshot of Disk Management on NV-DC1 showing the E: (DC1_Data) volume.

- **Evidence 6:** Screenshot of Disk Management on NV-FS01 showing the D: (NewVueData) volume.
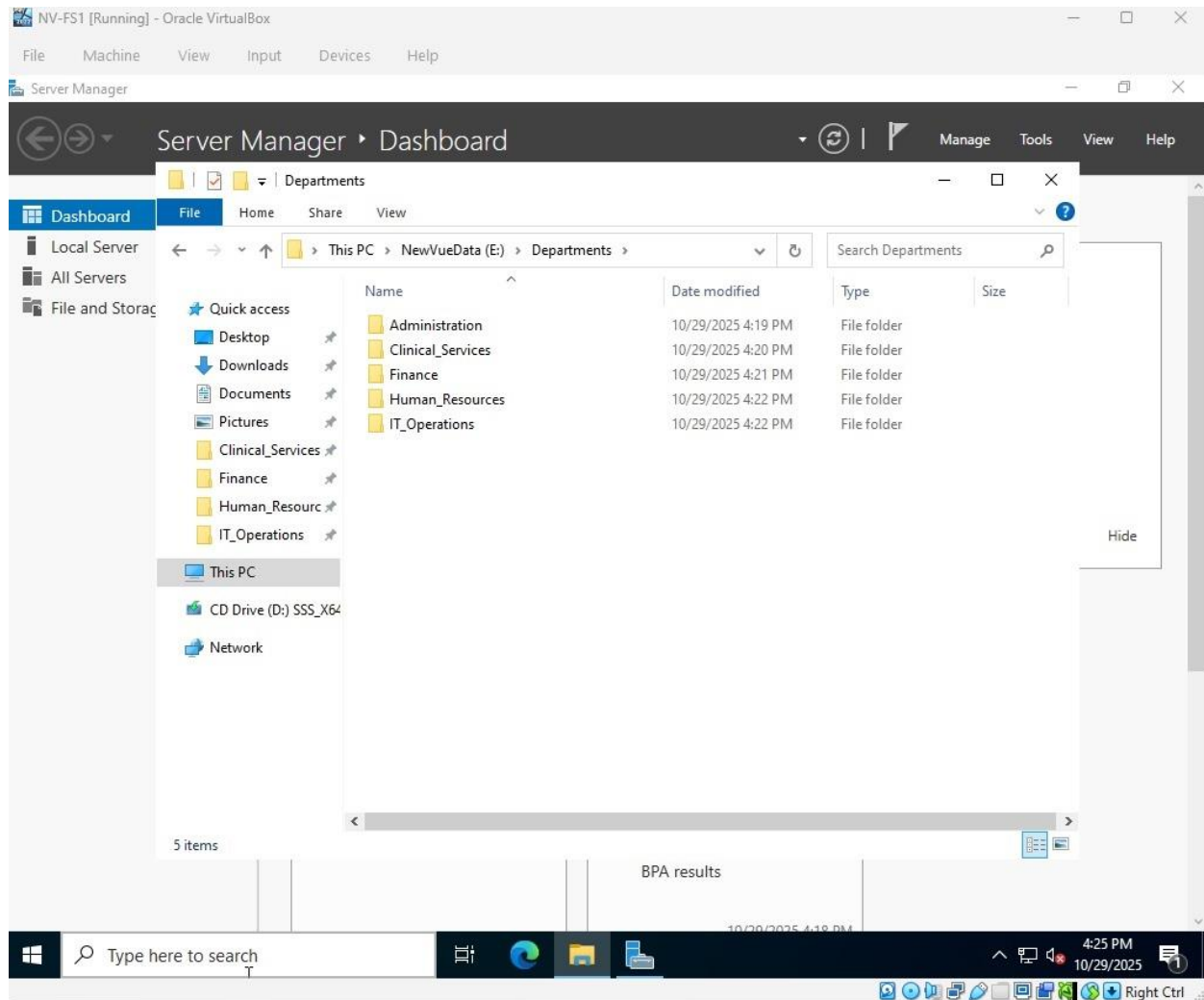
Section 3: Task — Departmental Folder Structure Creation (25 pts)

The storage drive on NV-FS01 was prepared with a hierarchical folder design that aligns with the organization's departments and functional units. A root folder named **Departments** was created, containing subfolders for each department and their respective functional units. This structure ensures clear data separation between organizational units. The table below shows the folder Structure.
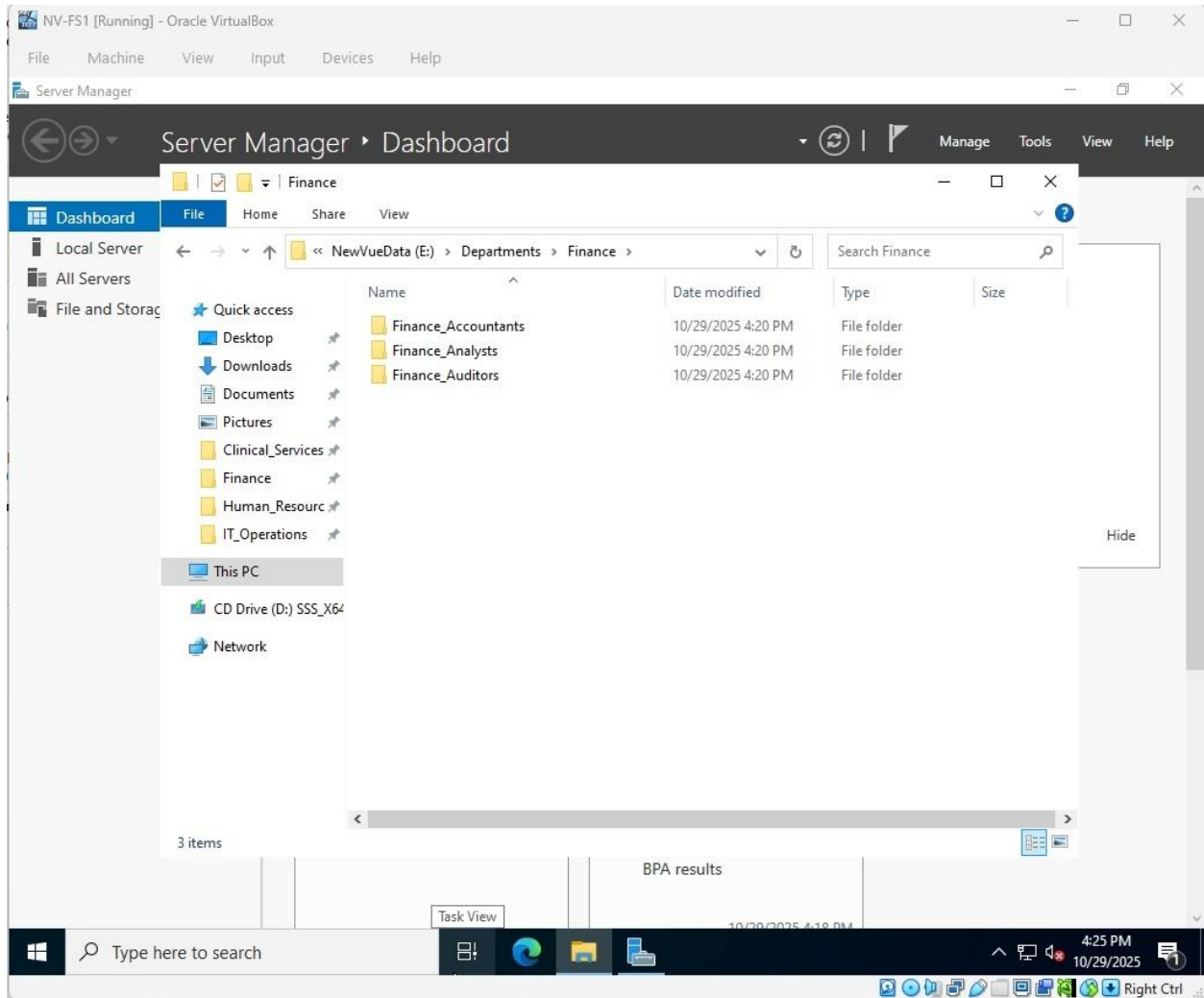
Root Folder	Departmental Folders	Sub folders
Departments	Administration	Admin_Managers, Admin_Clerks, Admin_Executives
	Clinical_Services	Clinical_Doctors, Clinical_Nurses, Clinical_Assistants
	Human_Resources	HR_Managers, HR_Recruiters, HR_Assistants
	IT_Operations	IT_Network, IT_Security, IT_Applications
	Finance	Finance_Accountants, Finance_Auditors, Finance_Analysts

Evidence

- **Evidence 7:** Screenshot of D:\Departments showing all department folders.

- **Evidence 8:** Screenshot of one department folder (for example, Finance) showing its functional subfolders.
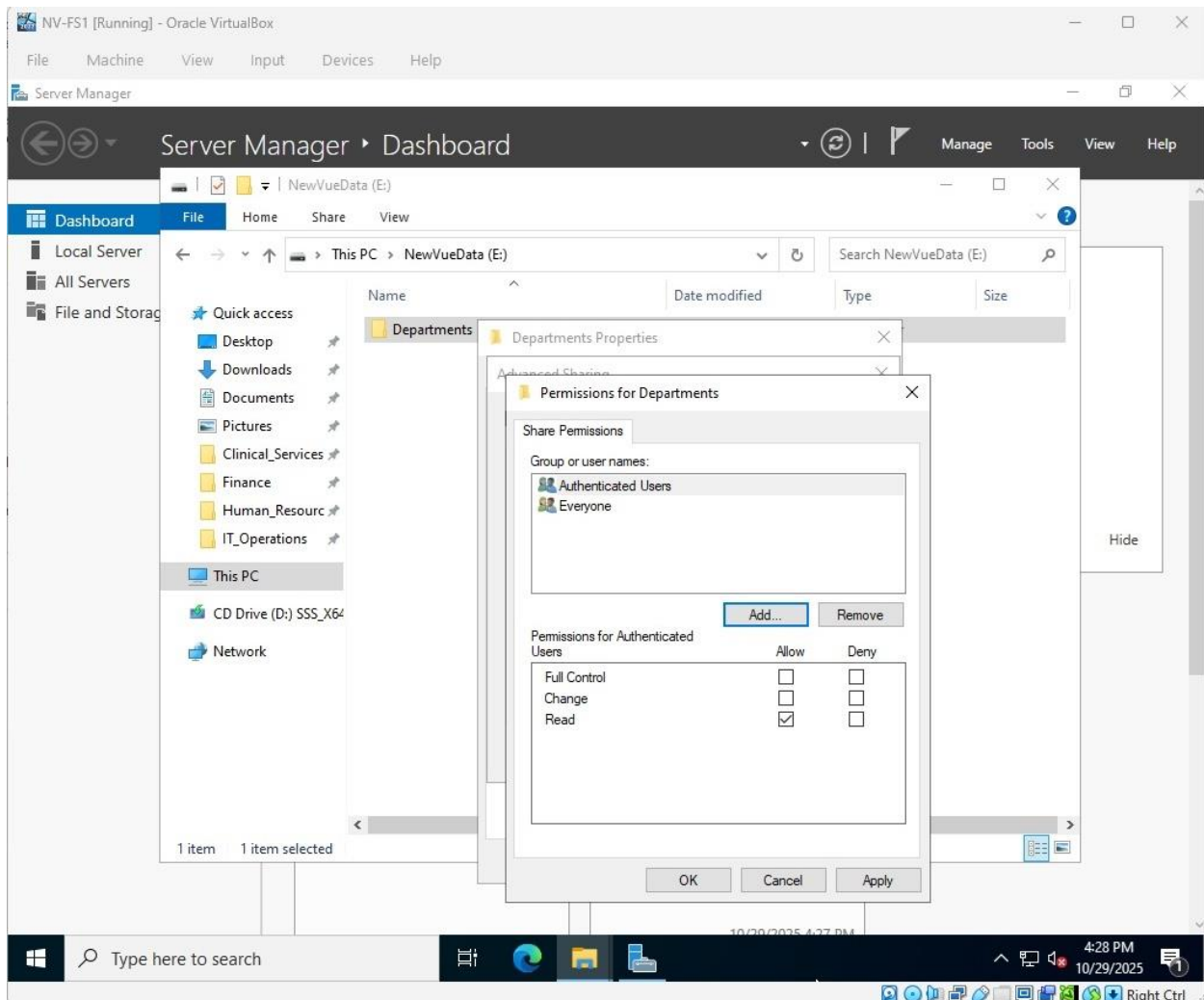
Section 4: Task — Sharing the Departments Folder (15 points)

The **Departments** folder was shared as a network resource to allow controlled access from domain clients. The share was configured under **Advanced Sharing**, granting **Read** permissions to **Authenticated Users** while removing the default **Everyone** group. This ensures only domain-authenticated users can browse the structure without altering shared data at the top level.

Evidence

- **Evidence 9:** Screenshot of the Advanced Sharing window showing Read permissions for Authenticated Users.

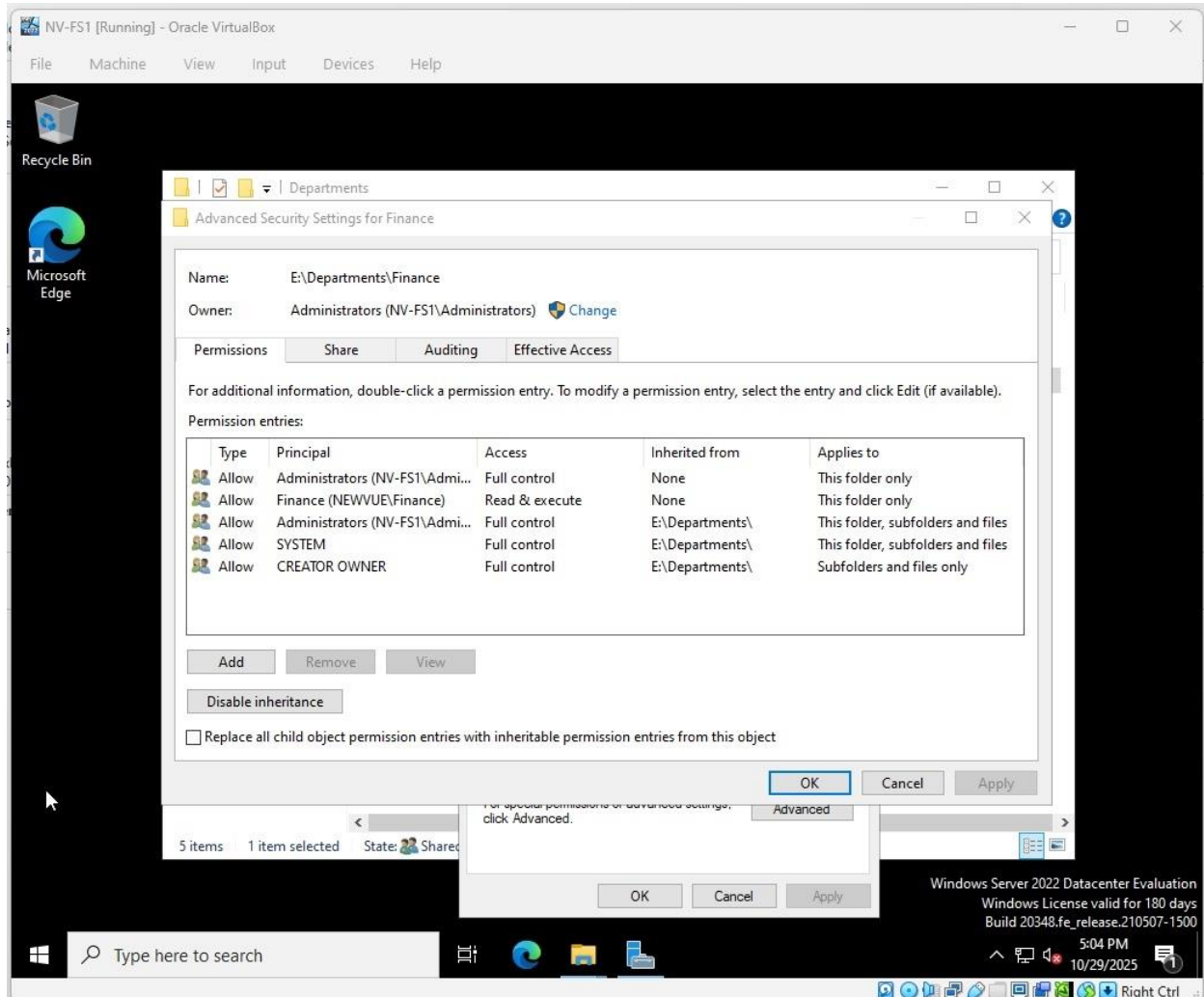# Section 5: Task - Applying NTFS Permissions (25 points)

NTFS permissions were configured to reflect organizational access requirements:

Briefly Describe how the ntfs permissions were configured for the root folder, departmental folders and the functional units.
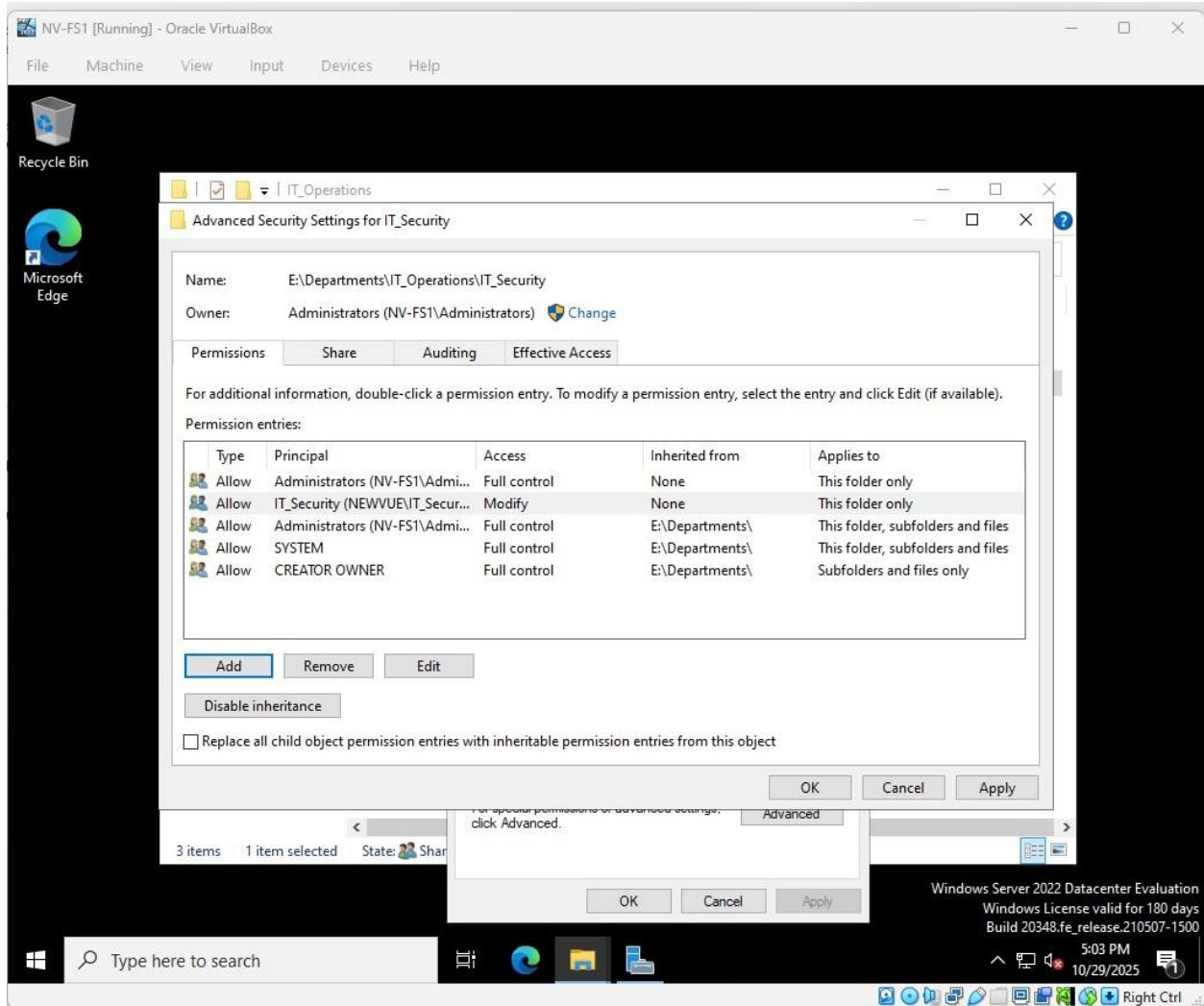
1. **Root Folder (D:\Departments):** The **Domain Users** group was granted **Read & Execute** permissions applied to **"This folder only."** This allows all authenticated users to see and browse the root Departments folder, but not to create files or folders directly within it.

2. **Departmental Folders (e.g., D:\Departments\Finance):** Each department folder (e.g., Finance) was configured with **Read & Execute** permissions for its corresponding departmental group (e.g., **Finance_Grp**), applied to **"This folder only."** This enables members to see their department's folder and access the functional subfolders within it, while preventing them from storing files directly in the main department folder.

3. **Functional Role Folders (e.g., D:\Departments\Finance\Finance_Analysts):** Each functional subfolder was granted **Modify** permissions for its specific functional group (e.g., **Finance_Analysts_Grp**). This gives the designated unit members the necessary rights to create, read, write, edit, and delete files within their own dedicated workspace.

Evidence

- **Evidence 10:** Screenshot showing NTFS permissions for one department folder (e.g., Finance) with *Read & Execute* permissions for its departmental group.

- **Evidence 11:** Screenshot showing NTFS permissions for one functional folder with Modify access assigned to the correct functional group.

Section 6: Task - Access Verification (15 points)

Verification was performed from the **NV-CL1** client by logging in with test accounts from various functional groups. Each user was able to open the root Departments share, view their departmental folder, and access only their respective functional folder, confirming correct NTFS and share permission inheritance.

Evidence

- **Evidence 12:** Screenshot showing access verification for at least one test user (successful or denied as expected).