**CTEC 305 Project 5 Report**

Rosemarie Kpaka

Bowie State University

CTEC 305 Server Administration 1

Professor Charles Wolford

November 21, 2024

**Introduction**

For this project, I implemented a Hyper-Converged Infrastructure (HCI) using VMware to centralize departmental file storage and access, ensuring high availability, fault tolerance, and scalability. This solution allows departmental collaboration through shared folders with strict access controls, ensuring that only authorized users can access their department’s data. The project involved creating and configuring a Windows Server 2022 VM, setting up data disks with RAID 5 for redundancy, creating department-specific folders, assigning permissions via Active Directory (AD), and verifying access controls.

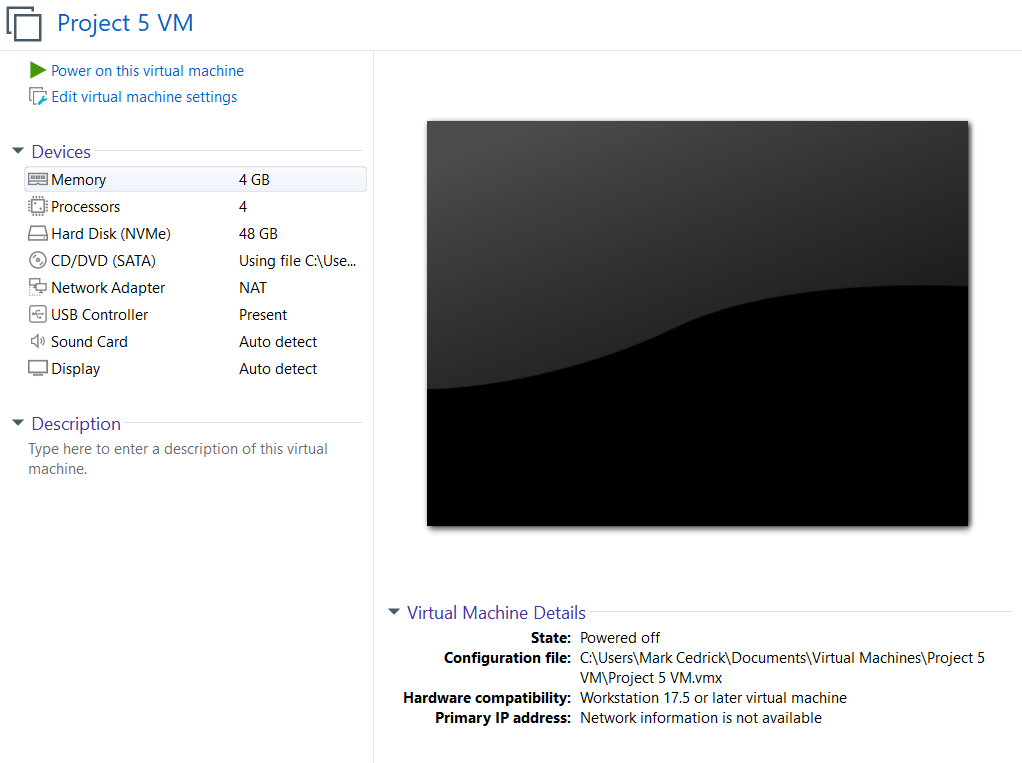
**Environment Setup**

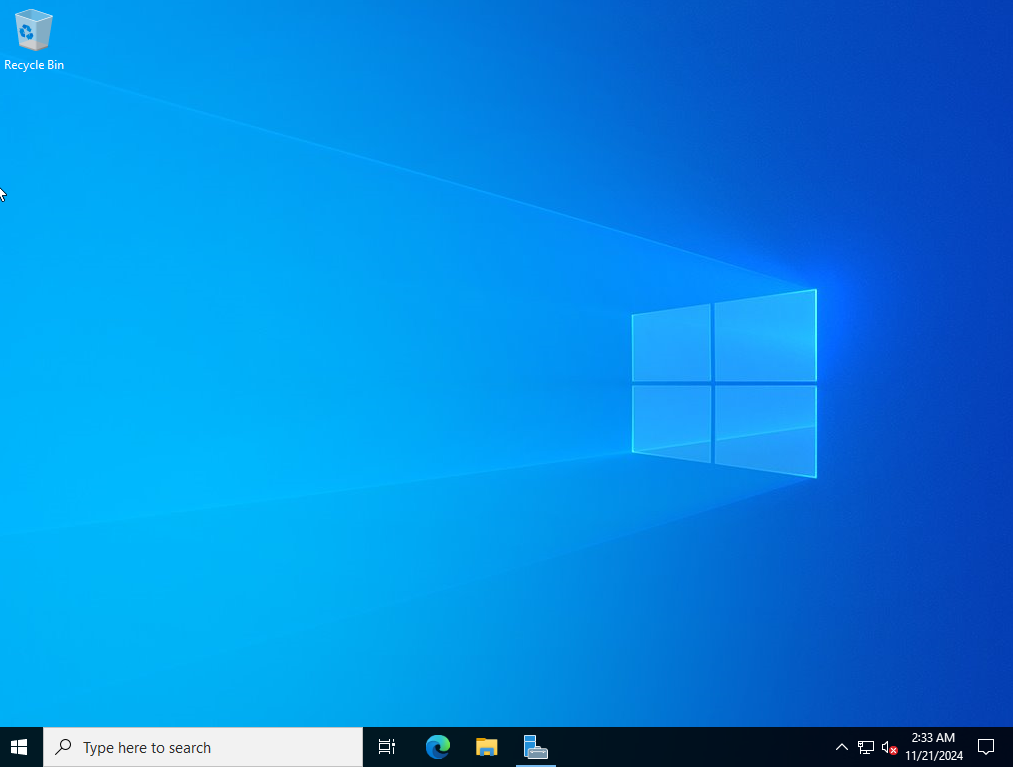
* Virtual Machines: 1 Windows Server 2022 VM
* Storage: 3 additional 10 GB data disks
* Roles/Features Used: Disk Management, Active Directory, File and Storage Services
* Platform: VMware Workstation
* Domain: rkdomain.local

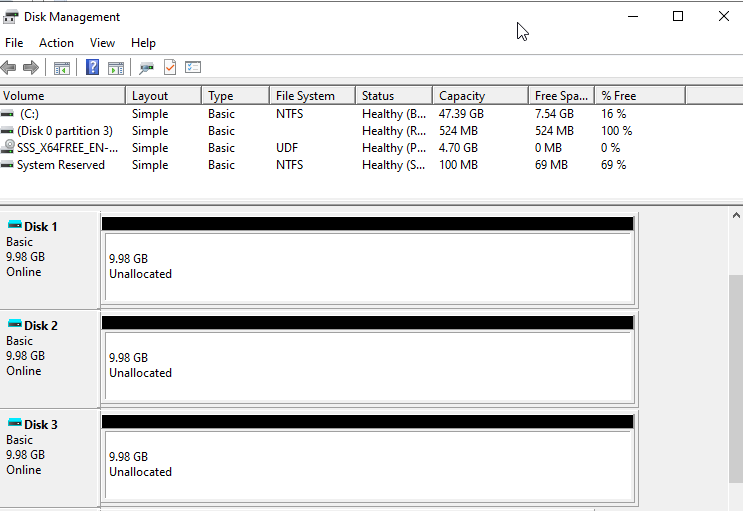
**Configuration Steps**

**Step 1: Create a Windows Server 2022 VM with Three Data Disks**

1. Opened VMware Workstation and created a new VM for Windows Server 2022 using a Custom (Advanced) configuration.
2. Assigned sufficient resources (2 CPUs, 4 GB RAM) and attached the Windows Server 2022 ISO.
3. Added three additional virtual disks of 10 GB each to simulate the required storage configuration (datadisk1, datadisk2, and datadisk3).
4. Installed Windows Server 2022 and ensured VMware Tools was installed for optimal performance.



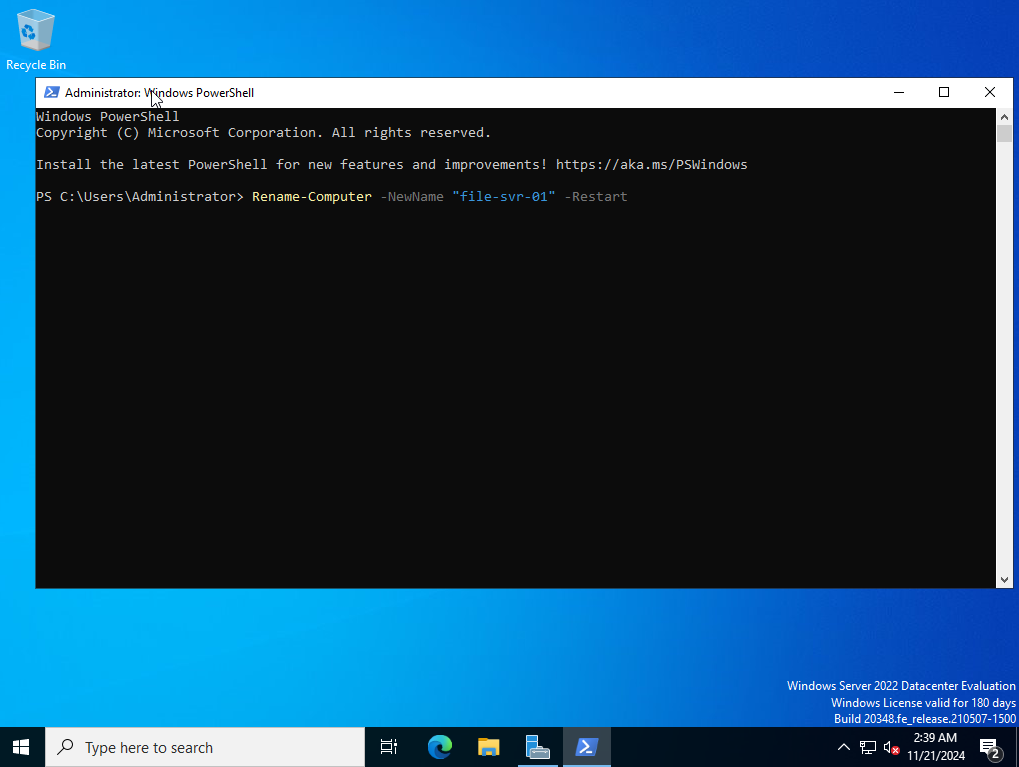




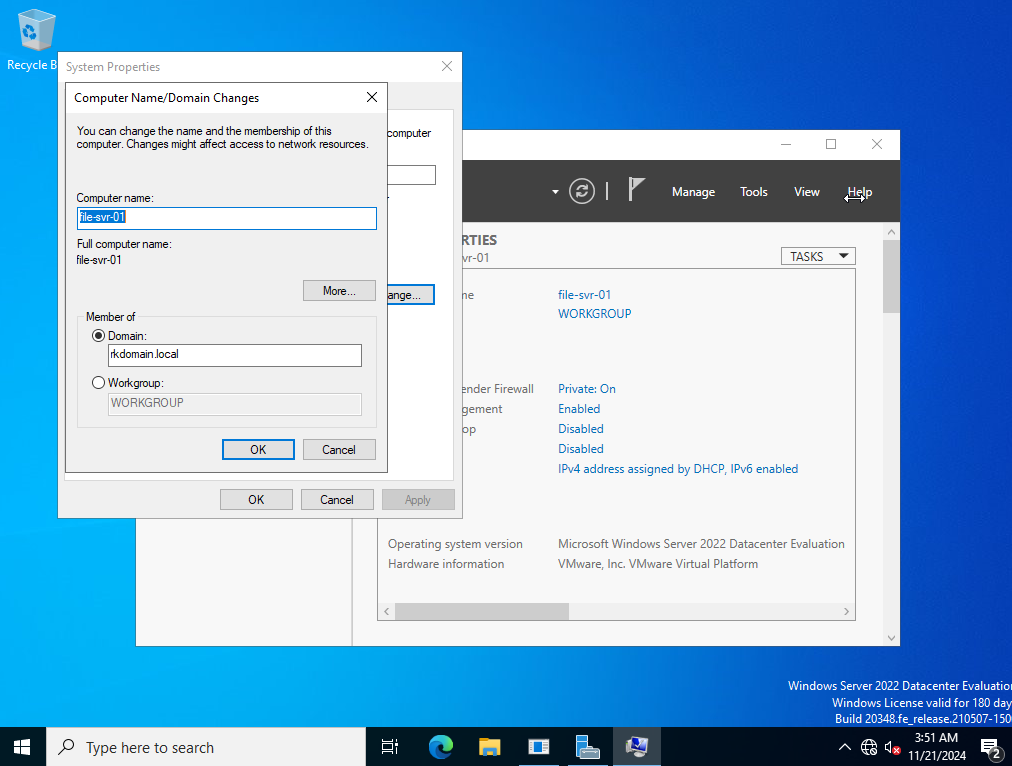
**Step 2: Rename the Server, Join the Domain, Assign Static IP, and Patch**

1. Renamed the server to file-svr-01 using PowerShell:

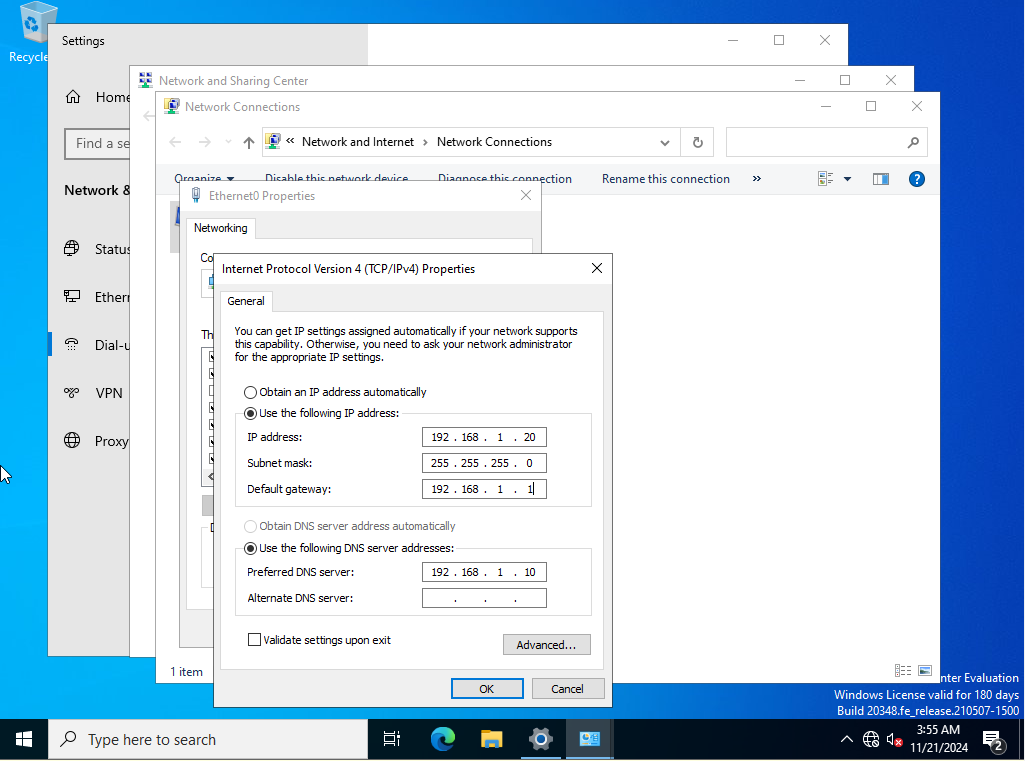
* Rename-Computer -NewName "file-svr-01" -Restart



1. Joined the server to the domain rkdomain.local through the Server Manager interface.

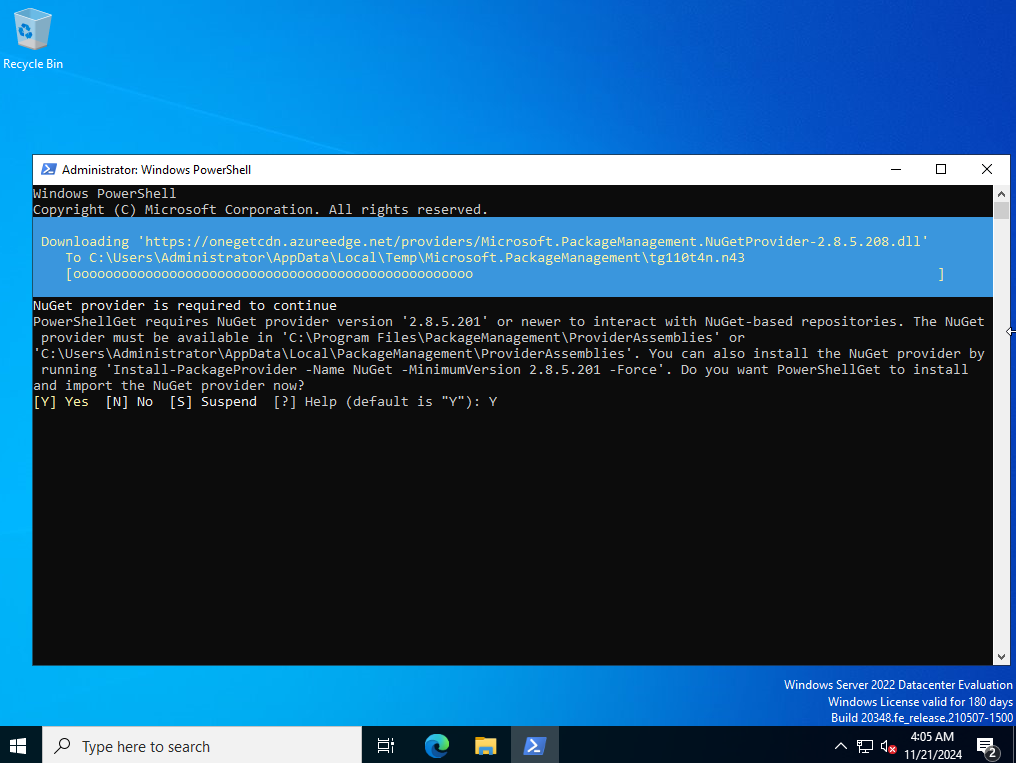


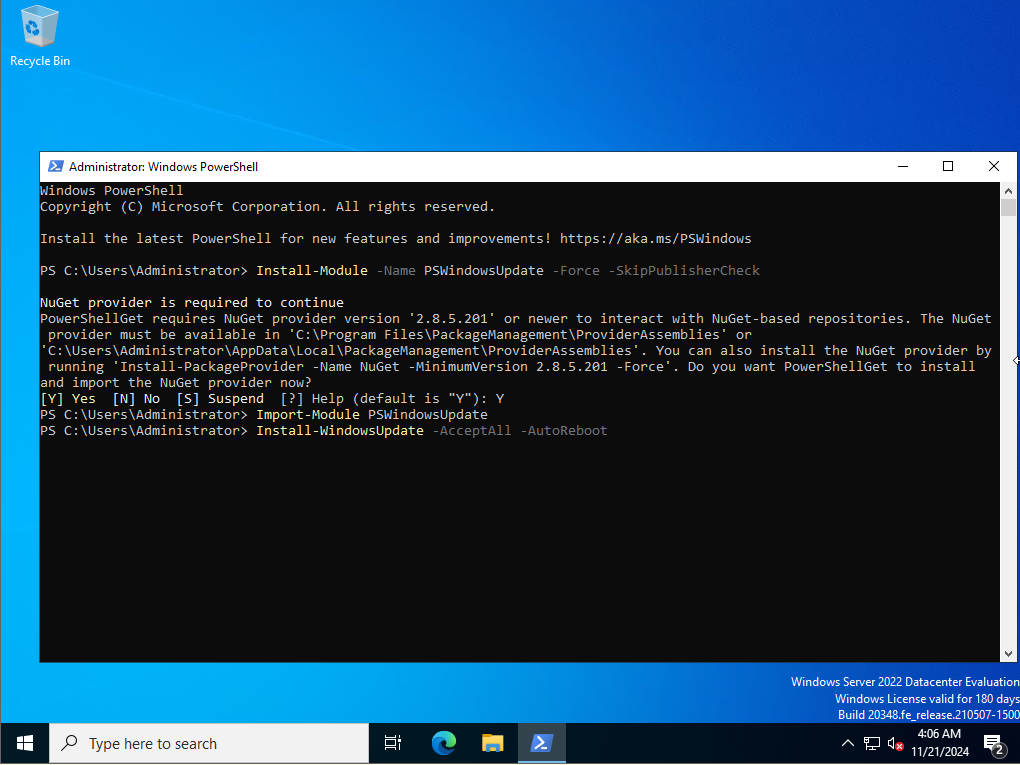
1. Assigned a static IP (192.168.1.20) using Network and Sharing Center, with DNS pointing to the primary domain controller (192.168.1.10).



1. Installed updates using the following PowerShell commands:

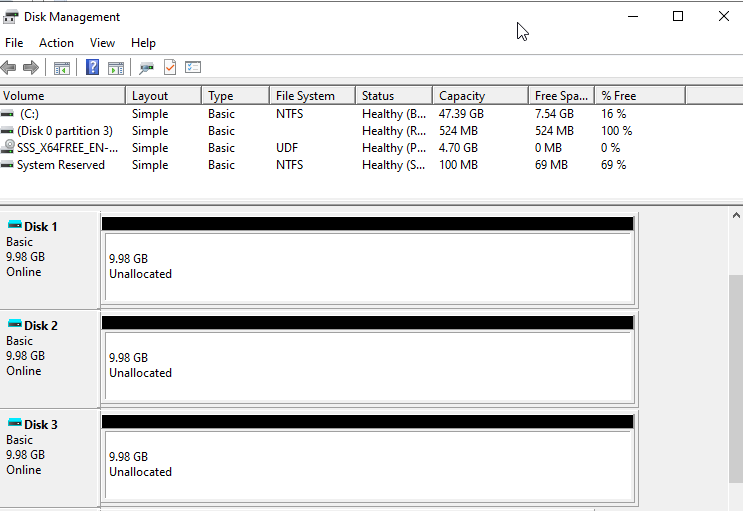
* Install-Module -Name PSWindowsUpdate -Force -SkipPublisherCheck
* Import-Module PSWindowsUpdate
* Install-WindowsUpdate -AcceptAll -AutoReboot





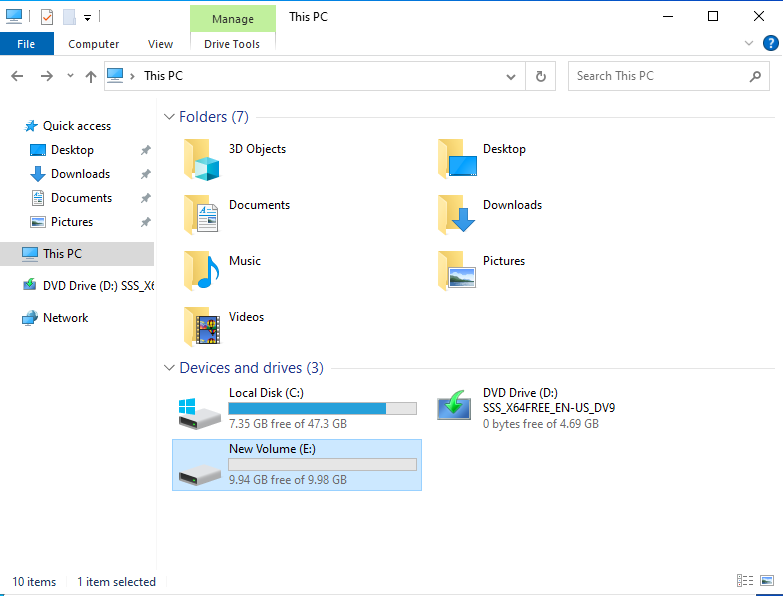
**Step 3: Initialize and Bring Data Disks Online**

1. Opened Disk Management on file-svr-01.
2. Brought datadisk1, datadisk2, and datadisk3 online.
3. Initialized the disks using the GPT partition style.



**Step 4: Configure Software RAID 5**

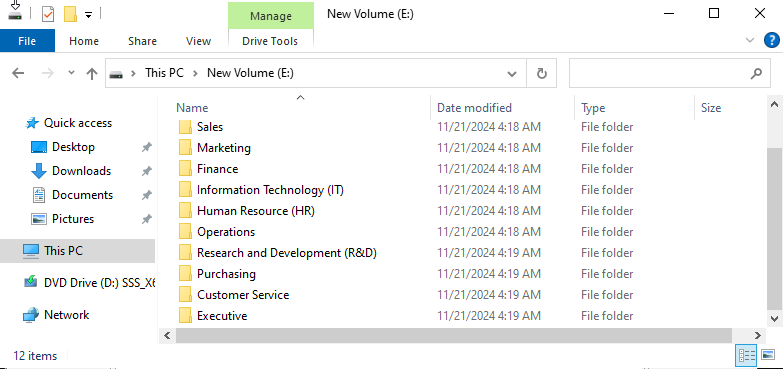
1. In Disk Management, right-clicked one of the initialized disks and selected New RAID-5 Volume.
2. Added the remaining two disks to the RAID array.
3. Assigned the drive letter E: and formatted the new volume as NTFS.
4. Verified the RAID 5 configuration provided redundancy across the three disks.

****

**Step 5: Create Department Folders**

1. Created folders on the RAID drive E: for each department:

* Sales
* Marketing
* Finance
* Information Technology (IT)
* HR
* Operations
* Research and Development (R&D)
* Purchasing
* Customer Service
* Executive

****

**Step 6: Configure NTFS Permissions and Share Folders**

1. Security Groups:

* Created security groups in Active Directory for each department (e.g., Sales Group, Marketing Group, etc.).
* Added department-specific users to their respective security groups.

1. Folder Permissions:

* Right-clicked each folder > Properties > Security tab.
* Added the corresponding security group with Full Control permissions.

1. Sharing Folders:

* Right-clicked each folder > Properties > Sharing tab > Advanced Sharing.
* Enabled sharing and assigned permissions to the respective security group.

**Step 7: Test Folder Access**

1. Logged into another domain-joined VM using test user accounts for each department.
2. Verified the following:

* Users could access their department’s folder.
* Users could not access folders belonging to other departments.

**Testing and Verification**

**Tests Performed:**

1. Logged in as SalesUser1 and verified access to the Sales share.
2. Logged in as MKTUser1 and verified access to the Marketing share.
3. Attempted cross-department access (e.g., SalesUser1 trying to access the Marketing share) and confirmed access was denied.
4. Verified RAID 5 functionality by temporarily taking one disk offline; data remained accessible, proving fault tolerance.

**Conclusion**

This project successfully implemented a Hyper-Converged Infrastructure (HCI) using a Windows Server 2022 VM with RAID 5. Departmental folders were created, secured, and shared with appropriate permissions. Testing verified that users could only access their respective department folders, ensuring data integrity and security. Through this project, I gained practical experience in configuring fault-tolerant storage solutions, setting up secure file-sharing environments, and managing access controls using Active Directory and NTFS permissions. This setup provides a scalable and reliable solution for departmental collaboration within the organization.