Securing Windows Server (Server Hardening)

Vatsal Patel

8980484

INFO8046

Wareez Bashorun

July 30, 2024

Table of Contents

Lab 1 - Securing Windows Server (Network Infrastructure Security) Lab

Description

This lab is designed to hone your configurations and security on a Windows Server environment using the practical application of Encrypted File System (EFS), Windows Firewall, and Audit Policies. You will know how to configure EFS regarding cryptographic features for files, how to design group policy and set up firewall rules for controlling the traffic, as well as organize complex audits for security threats. With practical activities, you will learn how to set access control for files, how to work with network security, and how to audit server works, which helps you to guarantee security for your Windows Server environment.

Observations

This lab on Windows Server Administration proved to be practical in providing exposure in improving the security of a server through different techniques including the Encrypted File System (EFS), Windows Firewall, and Audit Policies. In the case of EFS, they were able to show how files could be encrypted, and additional security added by characterized by the change in color representing the encrypted status of files or folders. The activity of configuring Windows Firewall to block ICMP traffic challenged the capacity of controlling the network traffic with ease; this exercise manifested with significant changes in the ping test when the configured rule was applied or removed. The main aspects of the audit policy configuration included monitoring and logging the events with the idea of being able to draw attention to security breaches as well as noting the need for auditing from all the users in a comprehensive manner to improve the established security measures. This approach of server hardening can be said to be 360-degree, or rather full-spectrum in securing the Windows Server environment.

Screenshots

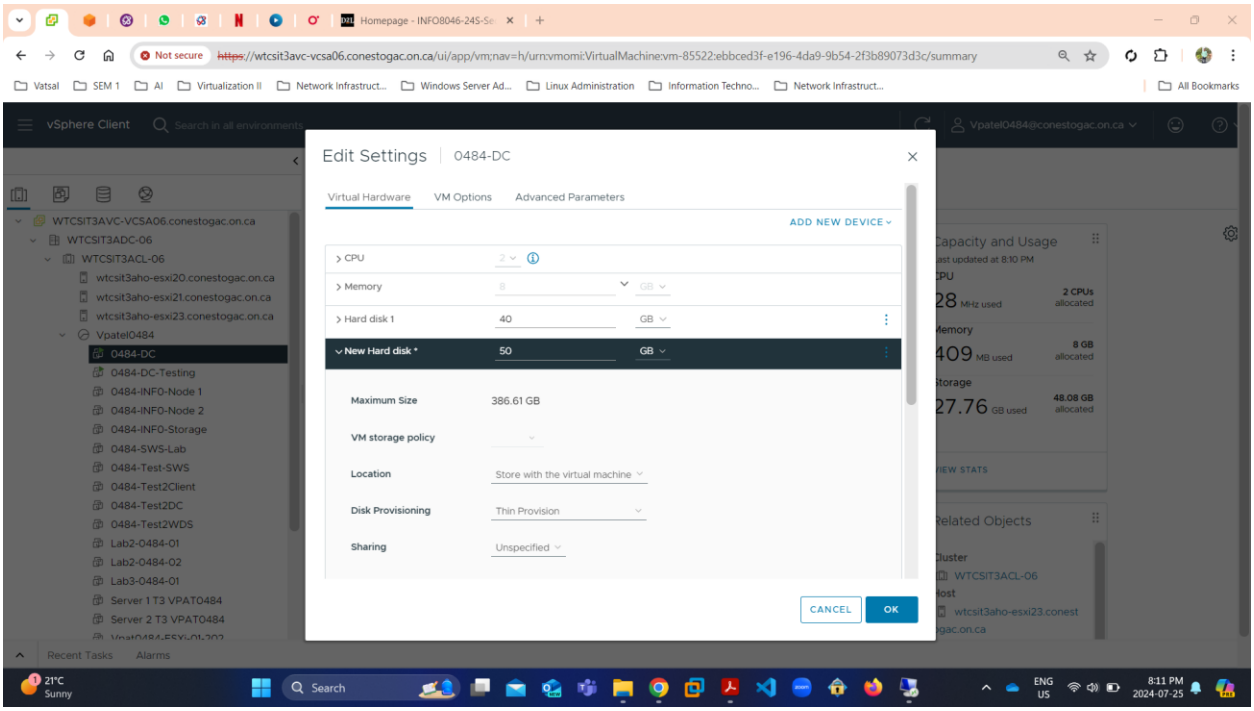

Fig 1: Picture shows adding another Hard Disk of 50GB in main domain controller 0484-DC.

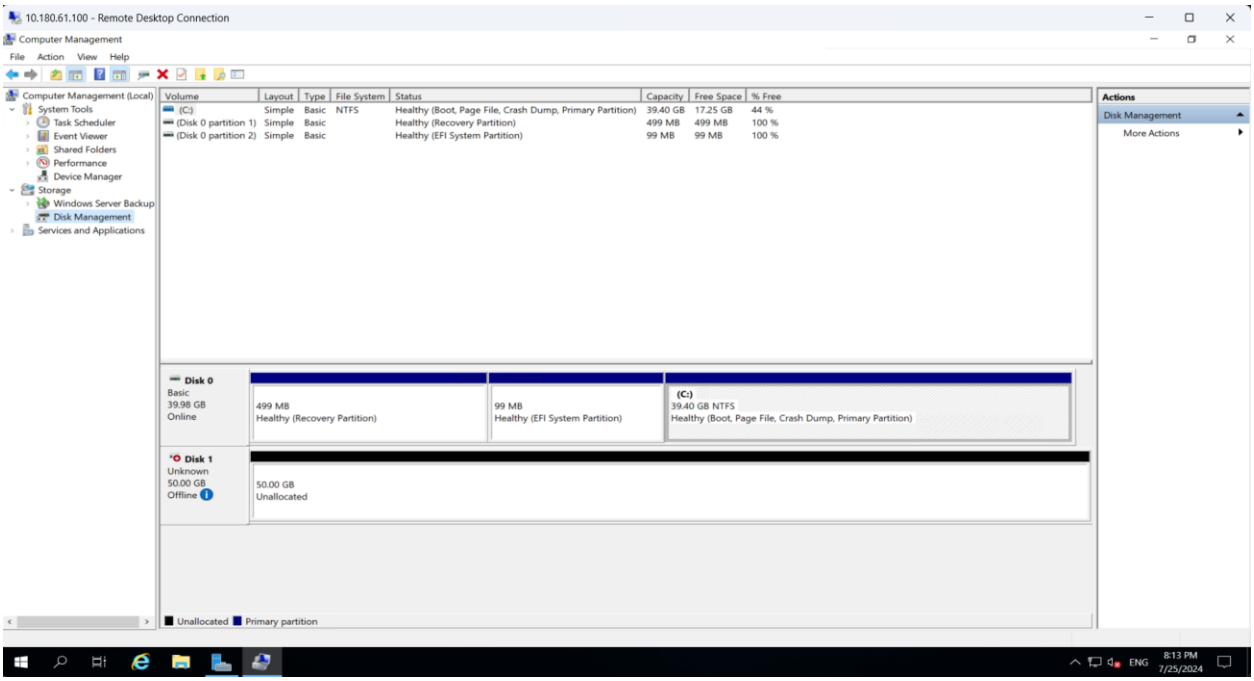

Fig 2: Picture shows Hard Drive successfully added into the virtual machine 0484-DC.

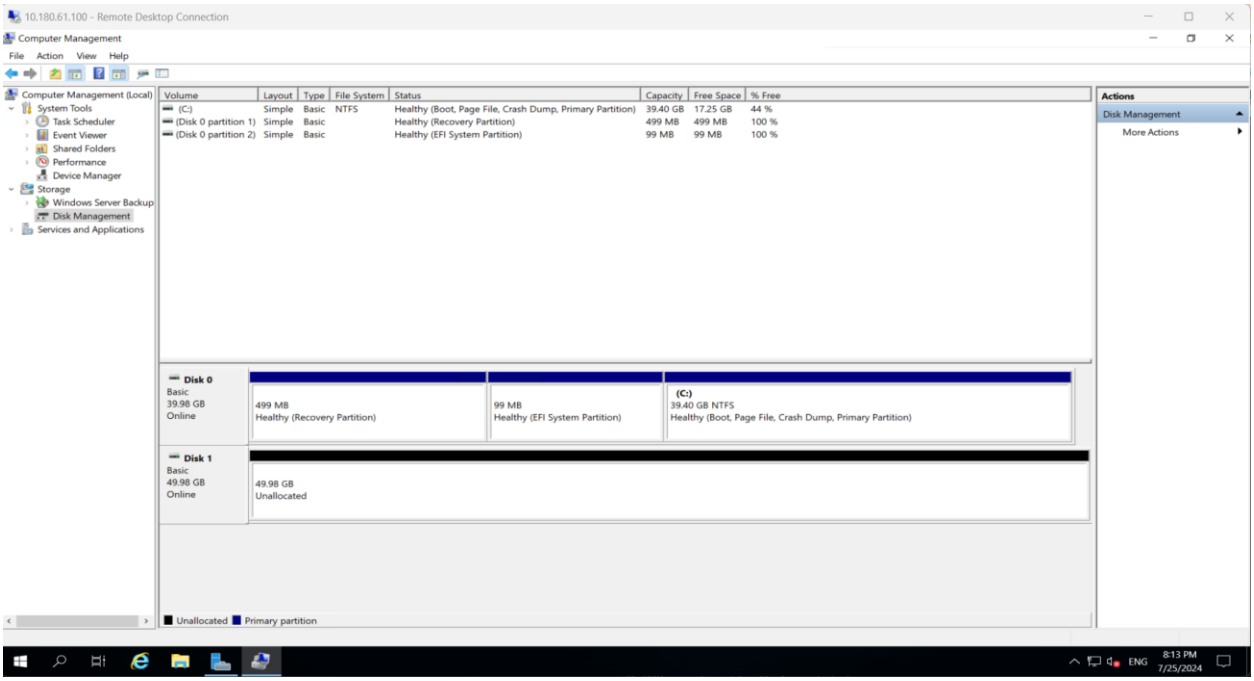

Fig 3: Picture shows initializing the disk and disk will be online successfully.

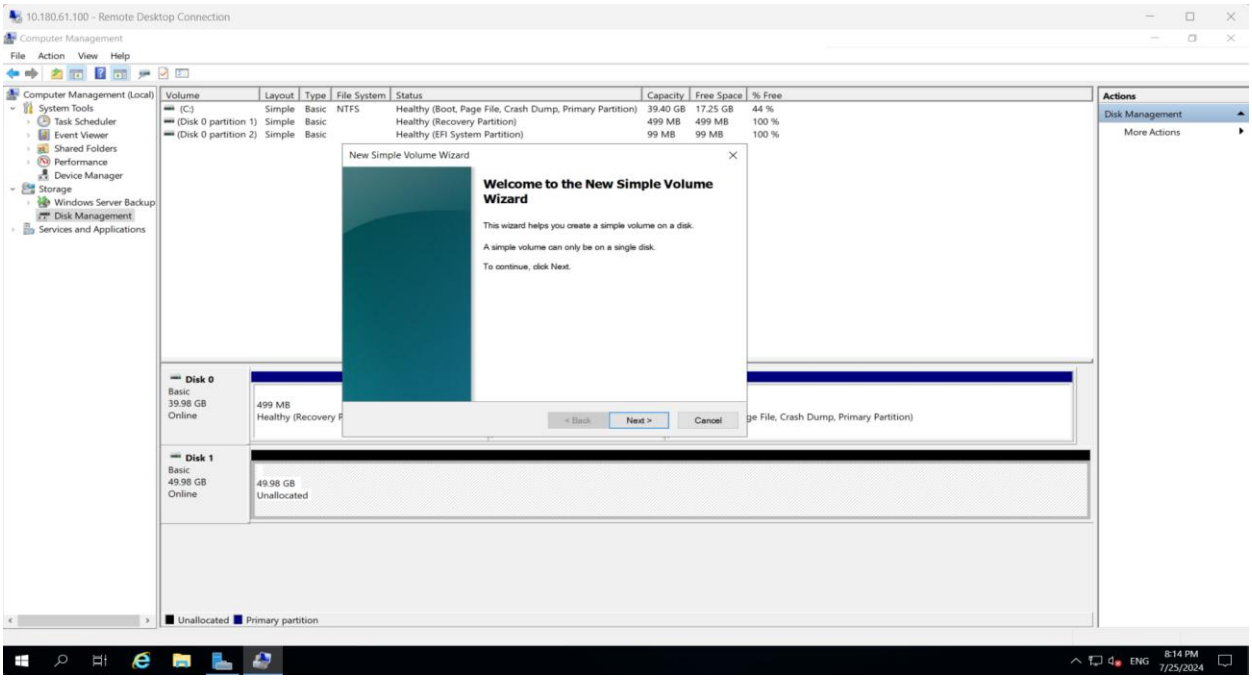

Fig 4: Picture shows creating the New simple volume wizards for the newly drive.

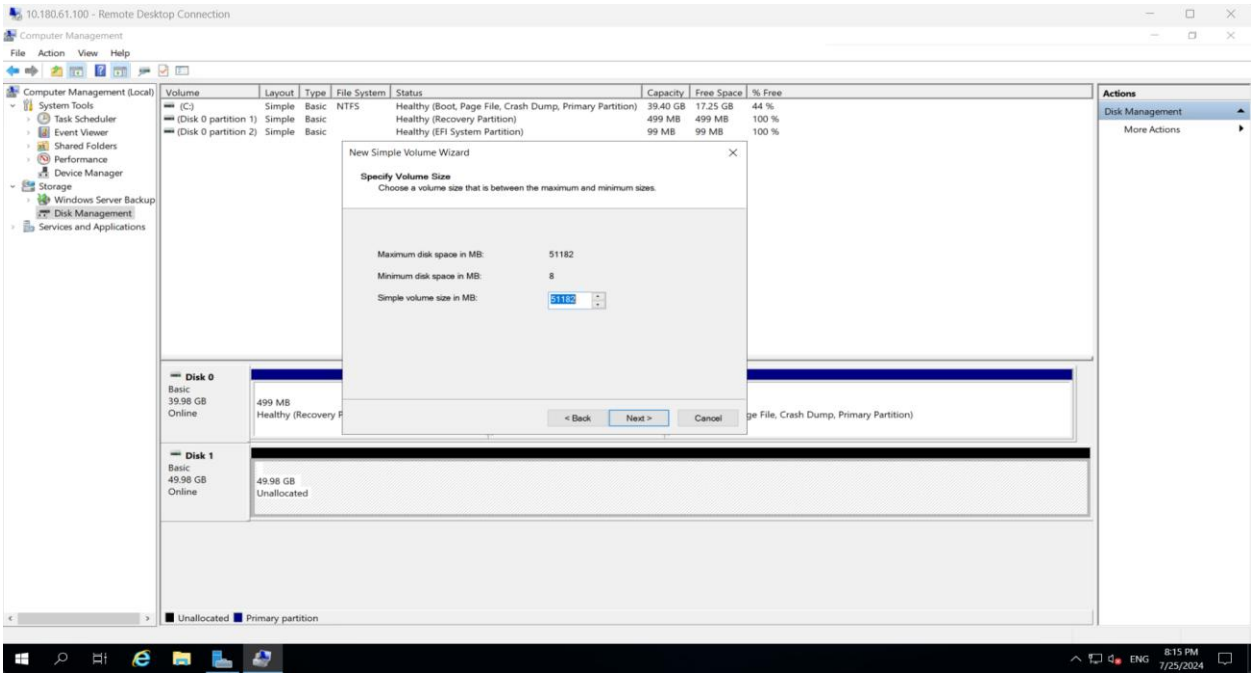

Fig 5: Picture shows specifying the volume size of the newly hard drive.

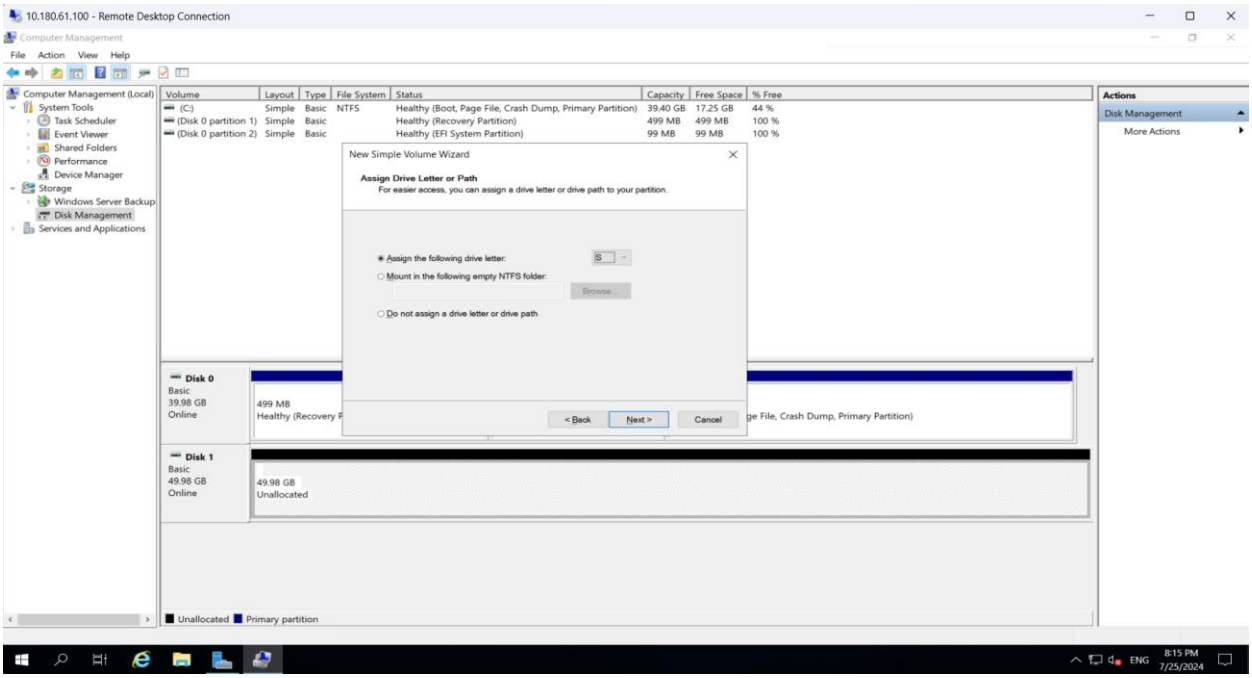

Fig 6: Picture shows given the drive letter S for the newly created drive.

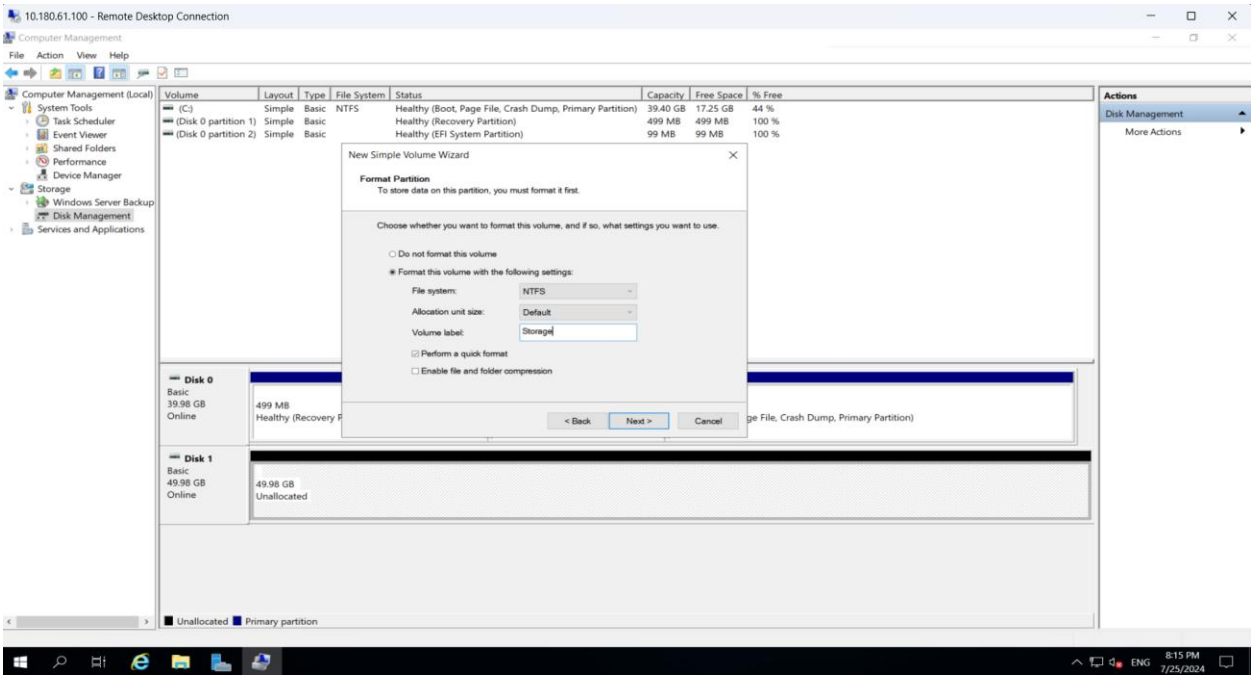

Fig 7: Picture shows the volume label which is Storage of the drive.

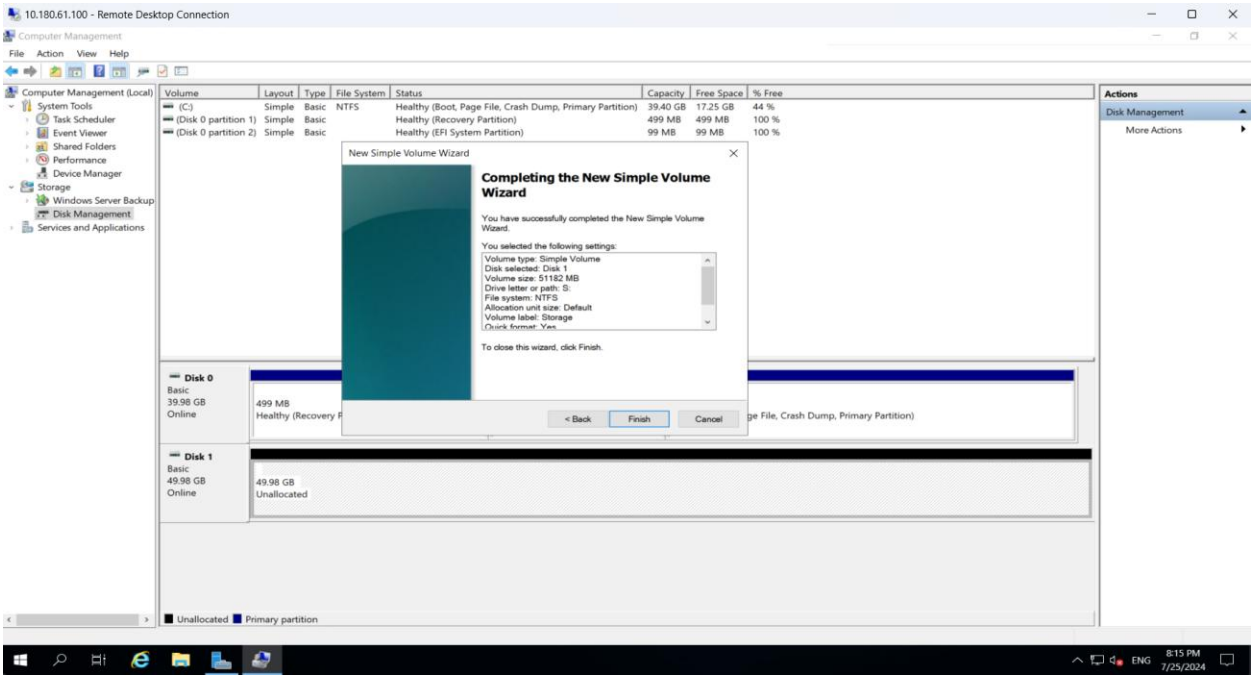

Fig 8: Picture shows successfully completed the new simple volume wizards.

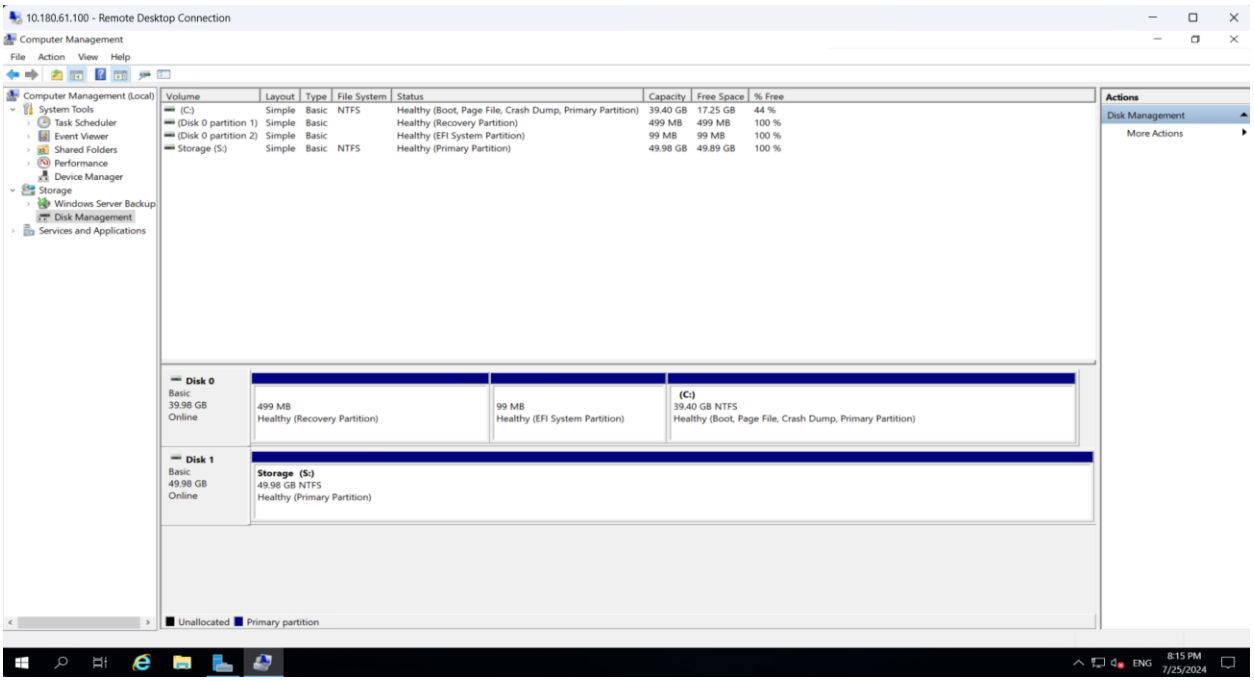

Fig 9: Picture shows the drive storage labeled by “S” successfully created.

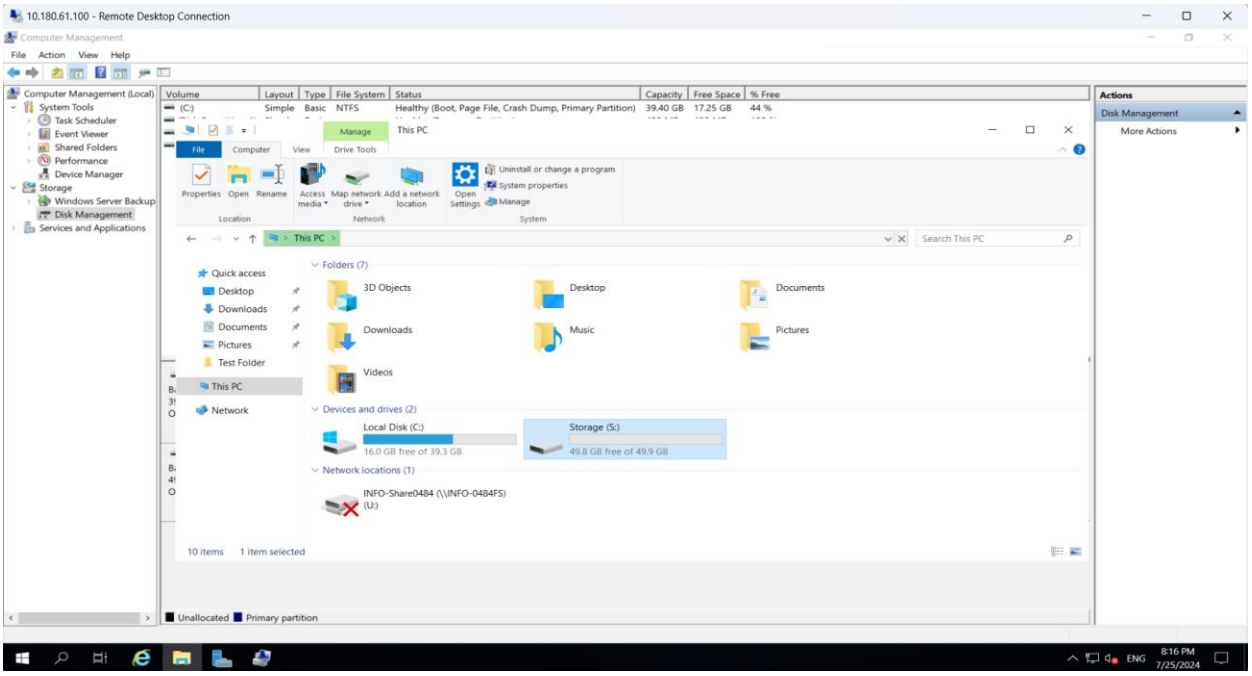

Fig 10: Picture shows the drive that we must create for the encrypted file system.

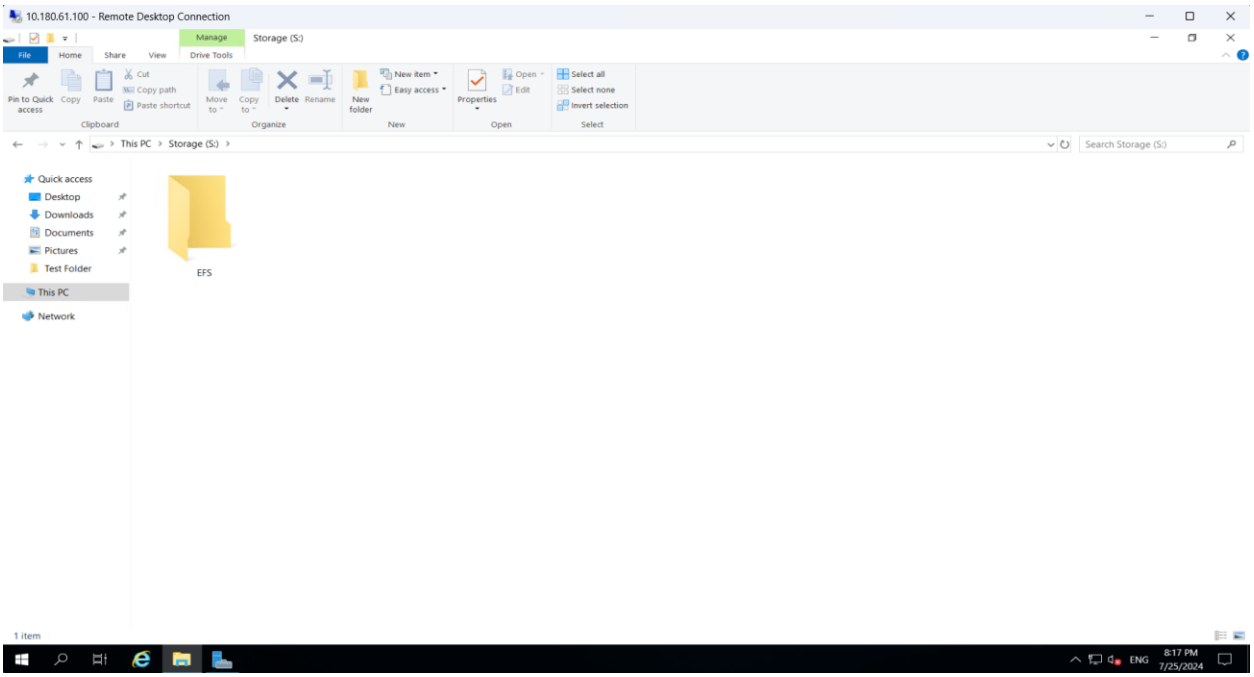

Fig 11: Picture shows creating a folder named EFS in the newly created drive.

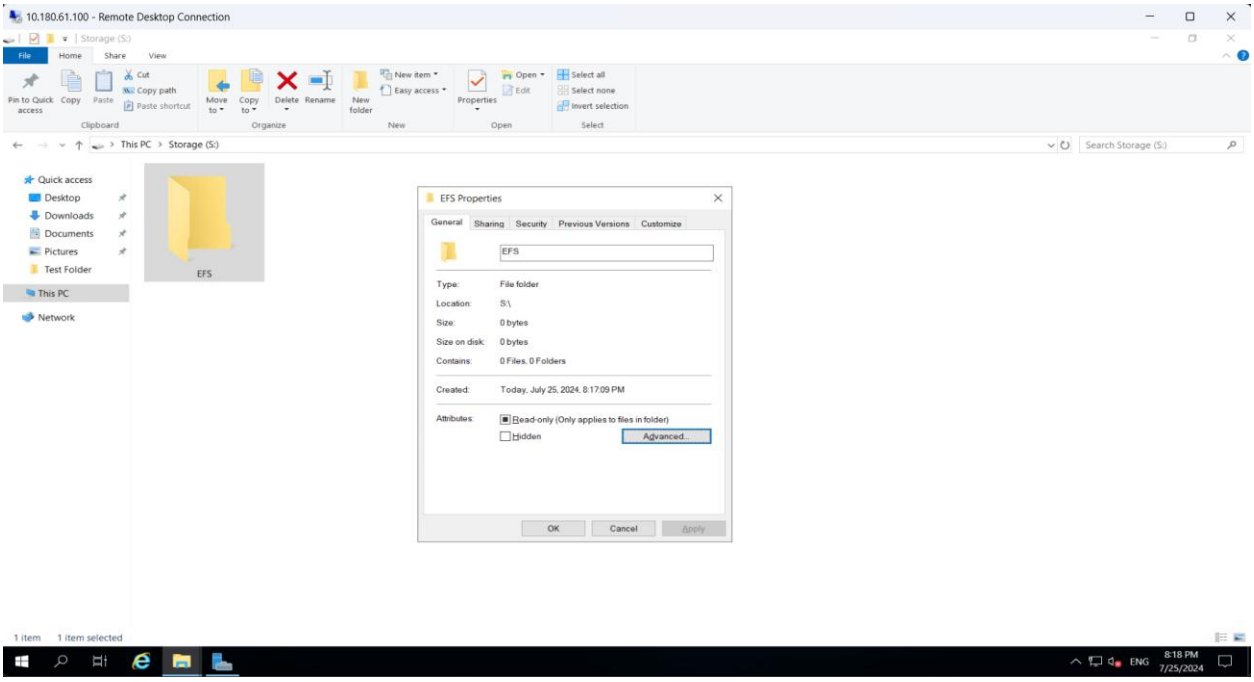

Fig 12: Picture shows EFS folder properties dialog box to encrypted them.

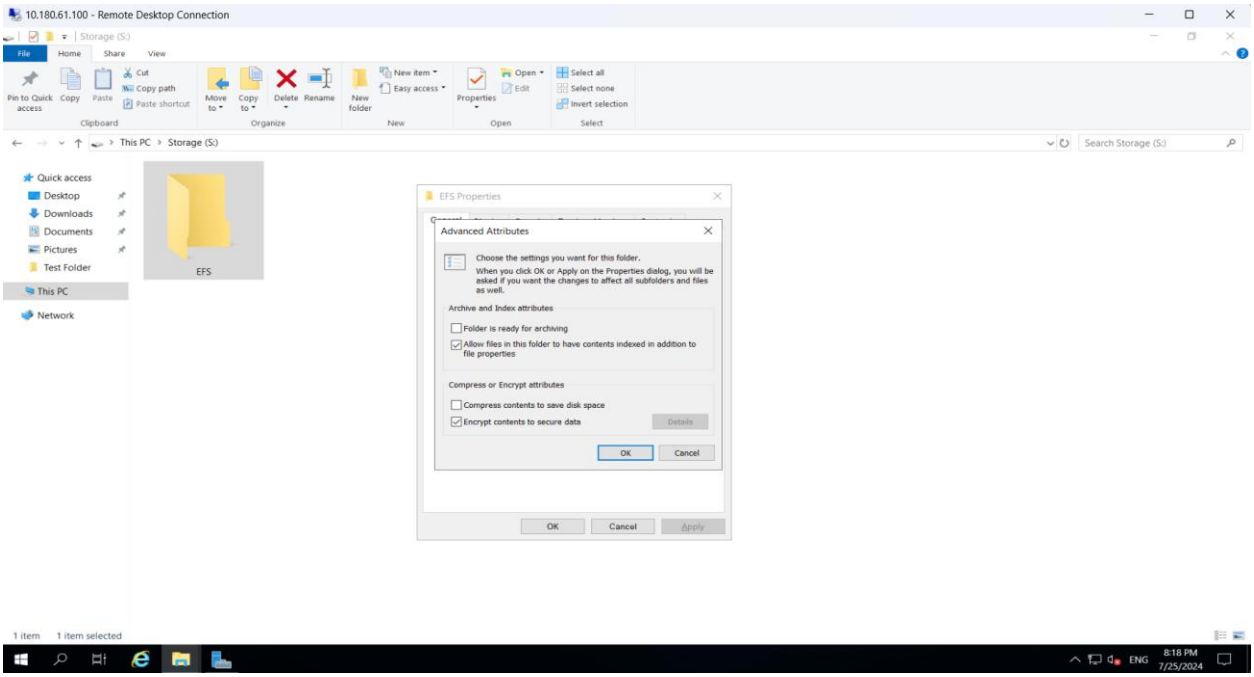

Fig 13: Picture shows to select the encrypt contents to secure data option in the compress or encrypt attribute.

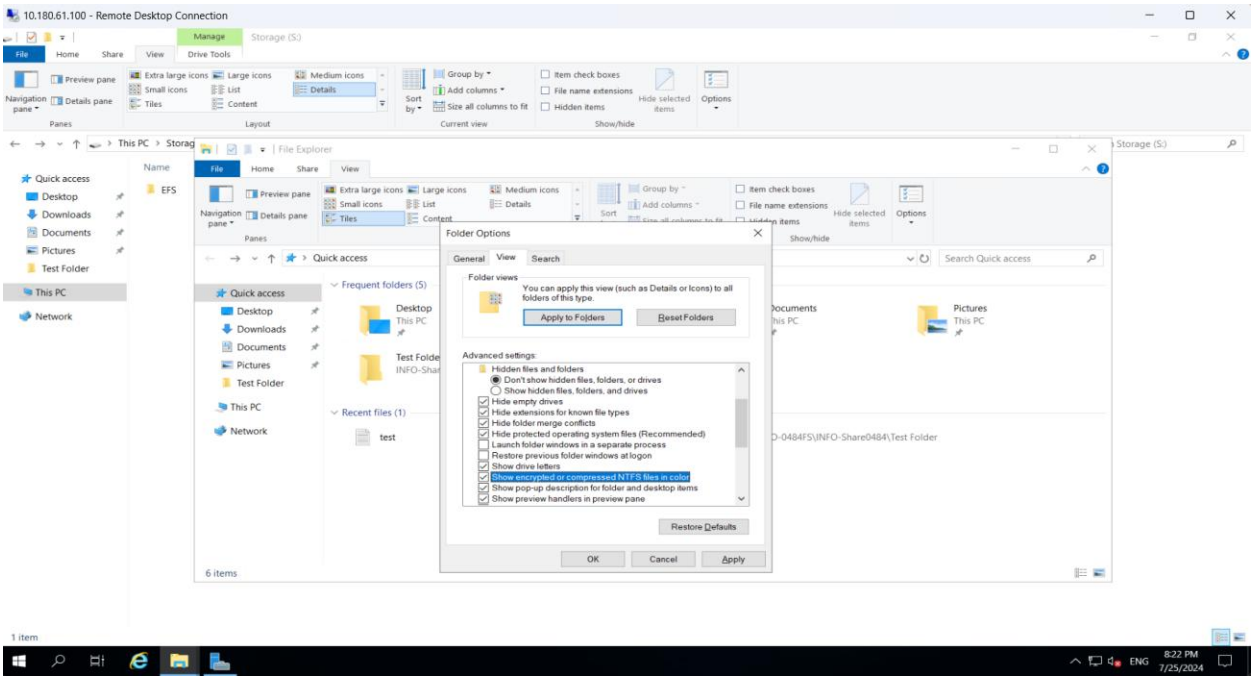

Fig 14: Picture shows confirming the setting to open the folder options to select the show encrypted or compressed NTFS files in color.

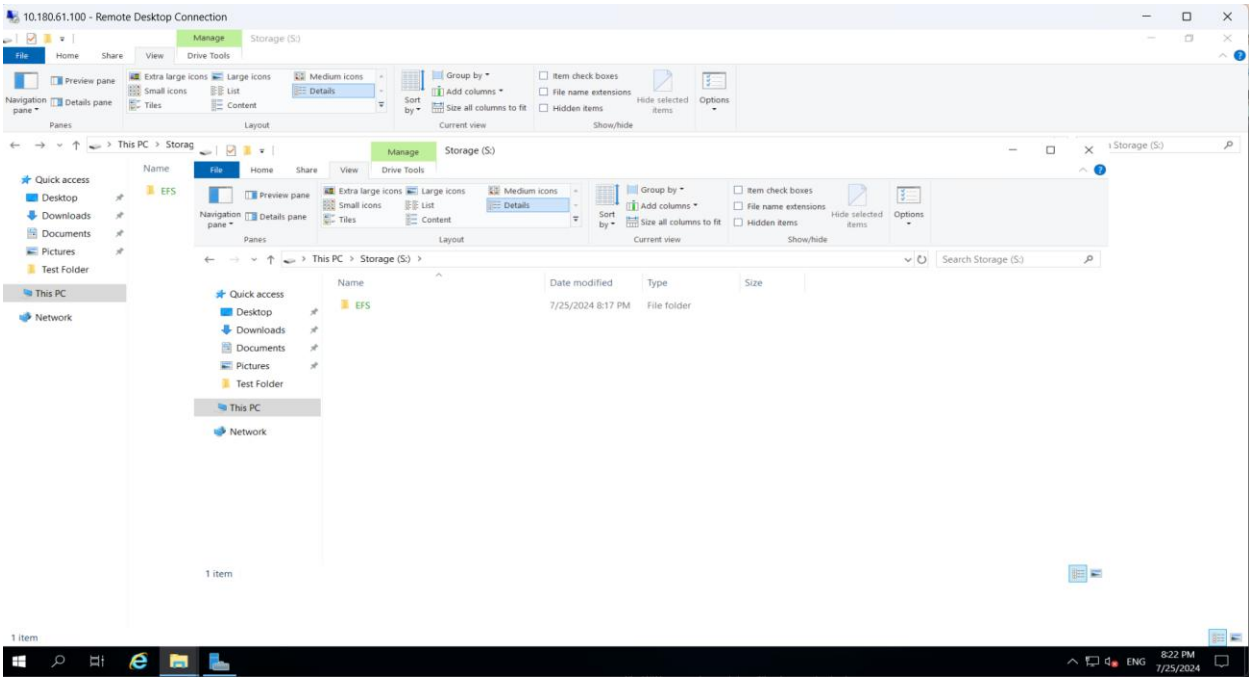

Fig 15: Picture shows the folder EFS Color is Green.

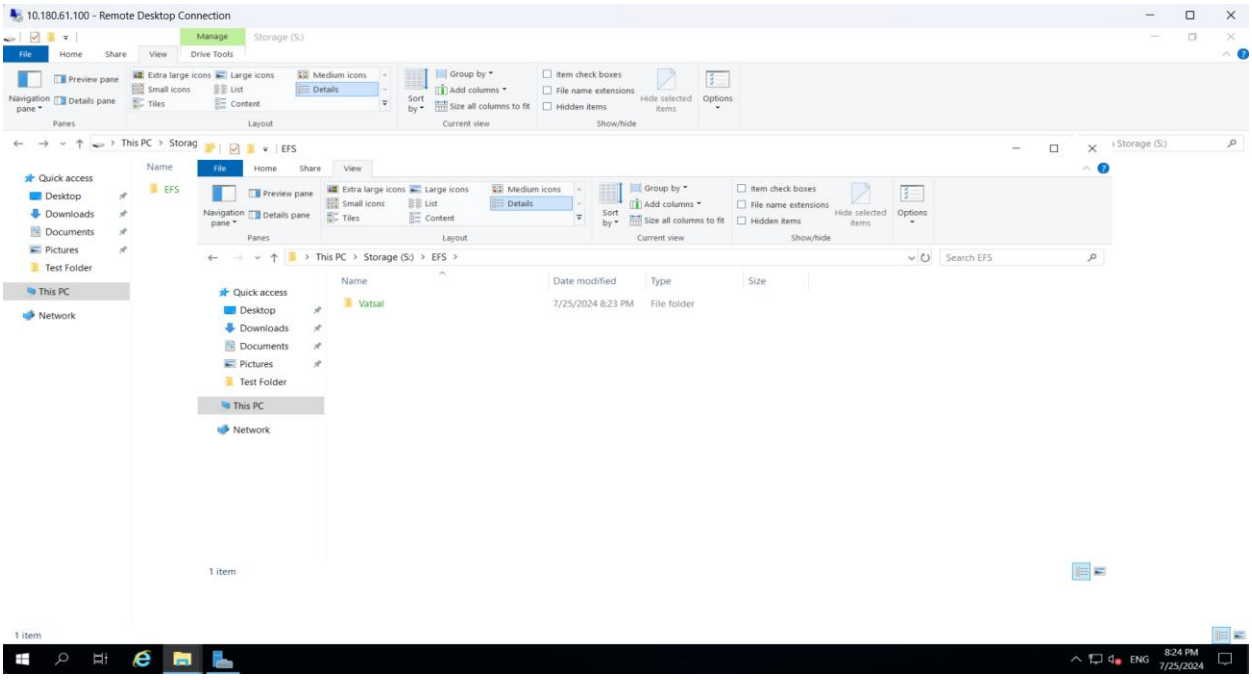

Fig 16: Picture shows adding another folder inside the EFS which will also be green color.

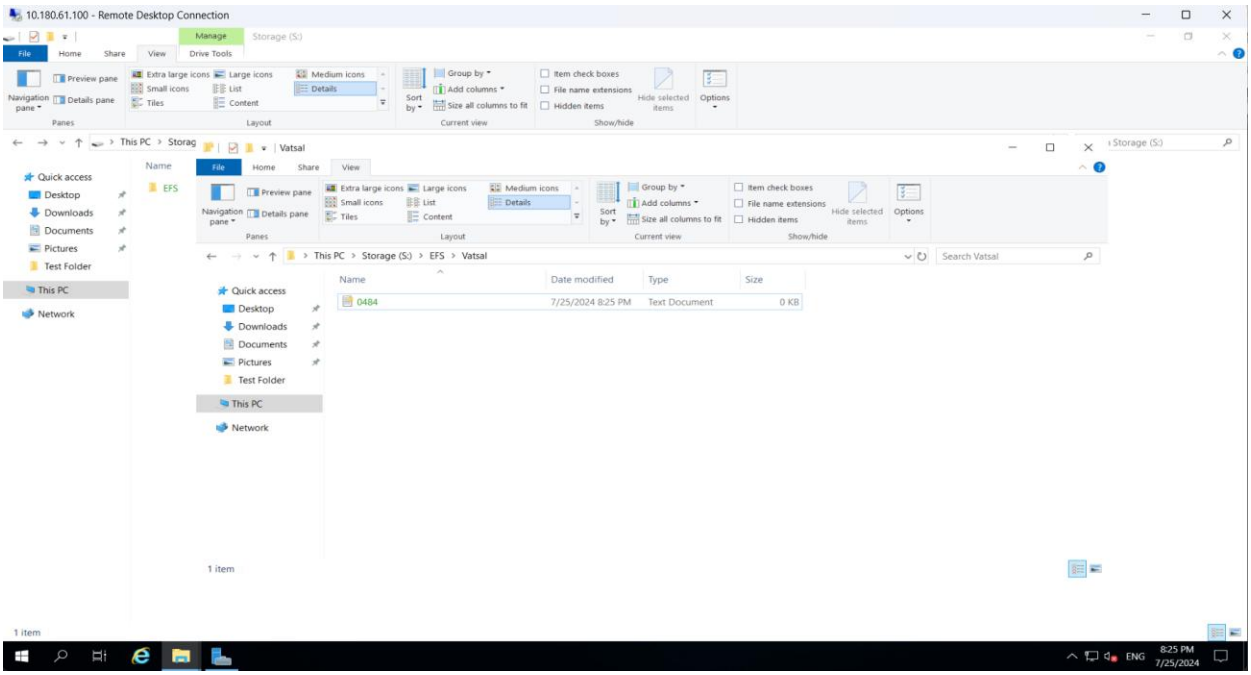

Fig 17: Picture shows adding the file inside the newly created folder which will also be Green.

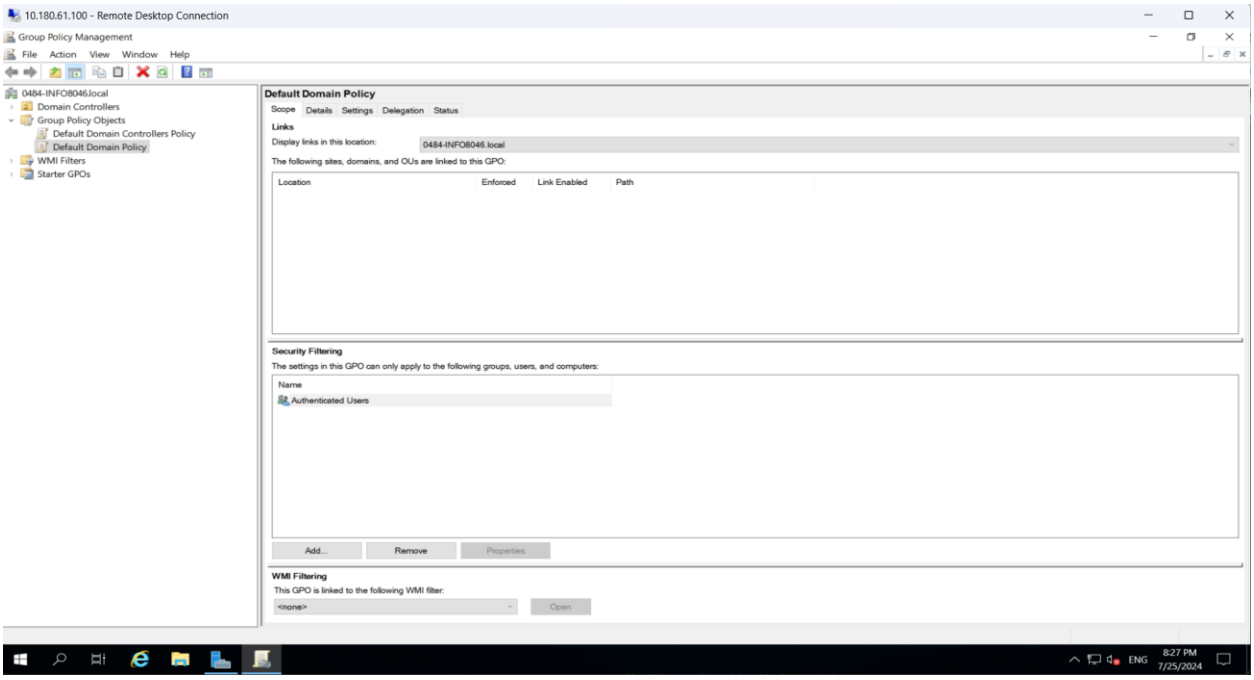

Fig 18: Picture shows opening the group policy management in the main domain controller.

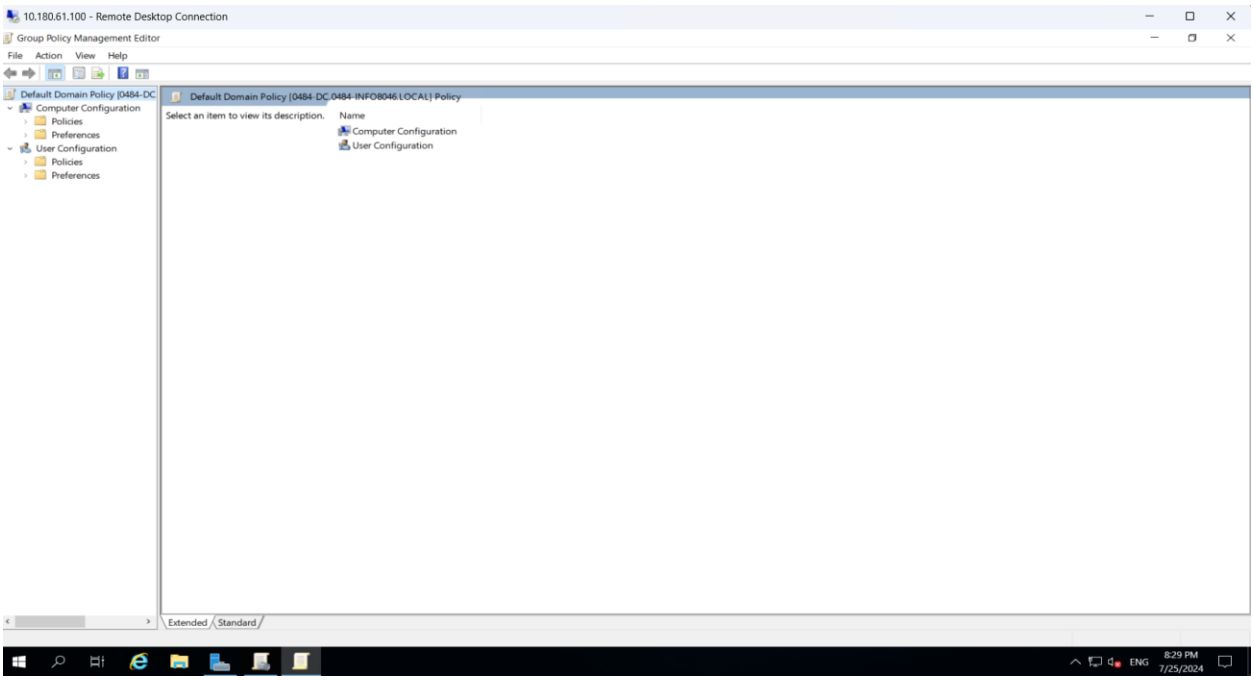

Fig 19: Picture shows open the default domain policy into the Group Policy Management.

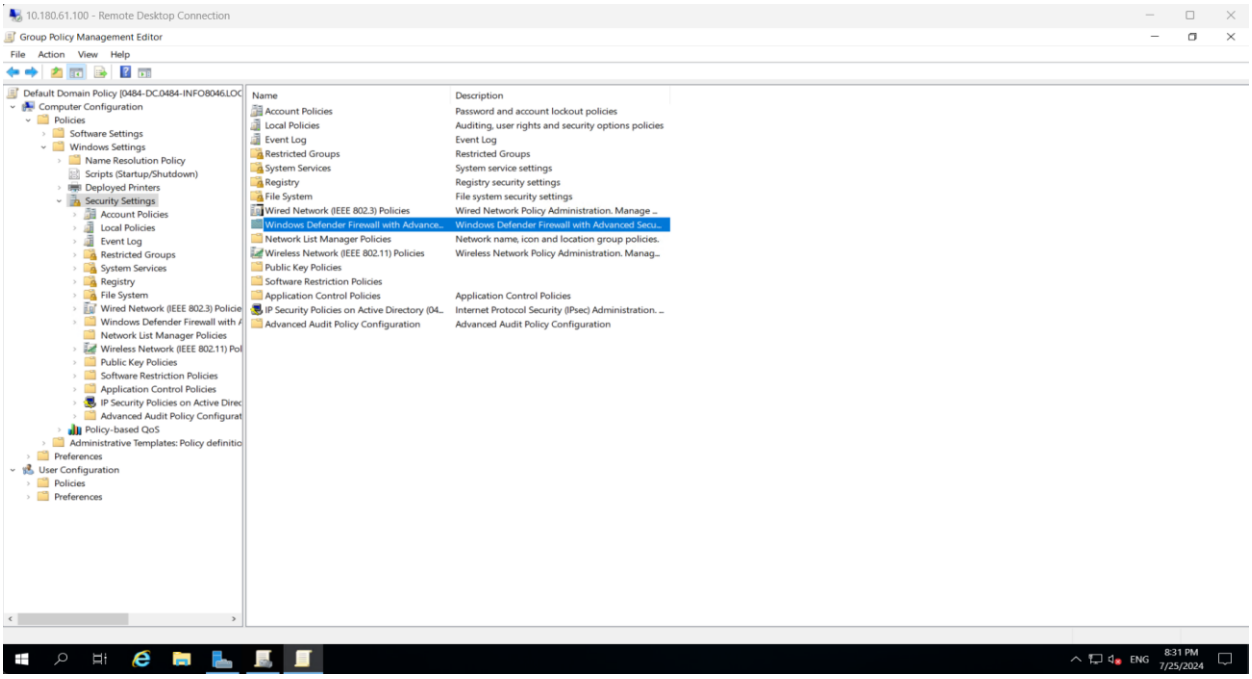

Fig 20: Picture shows navigating the Windows Defender Firewall with Advanced Security.

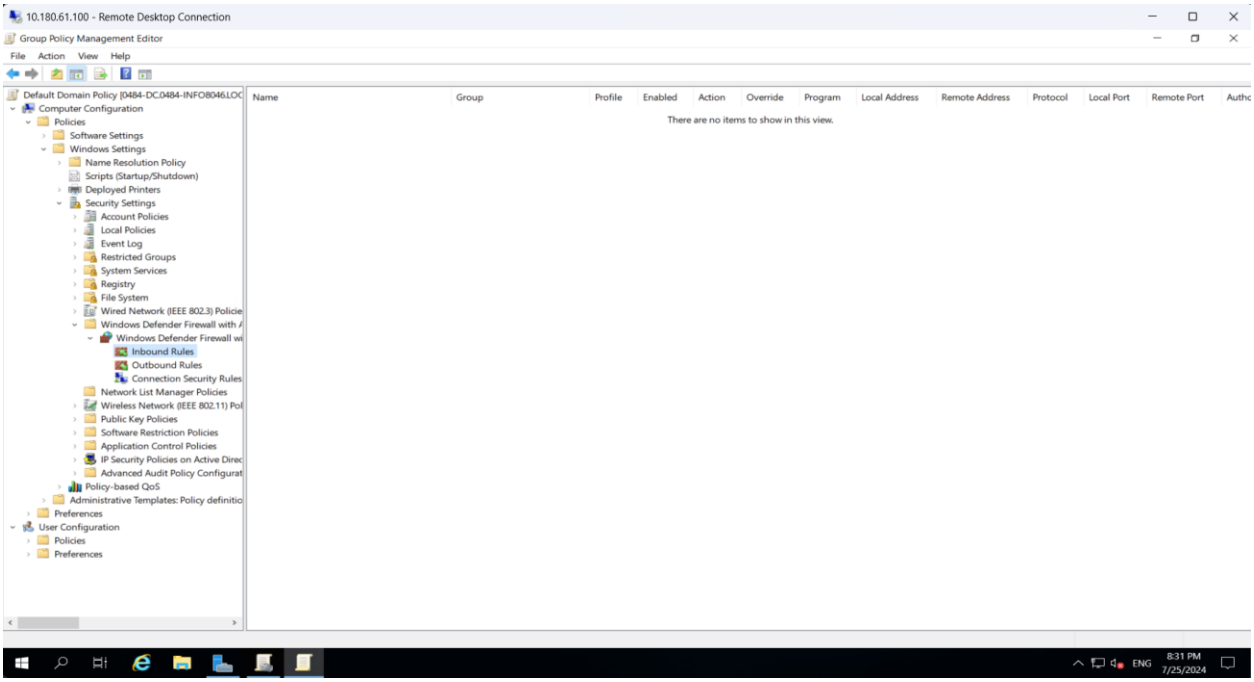

Fig 21: Picture shows selecting the inbound rules inside the Windows defender firewall.

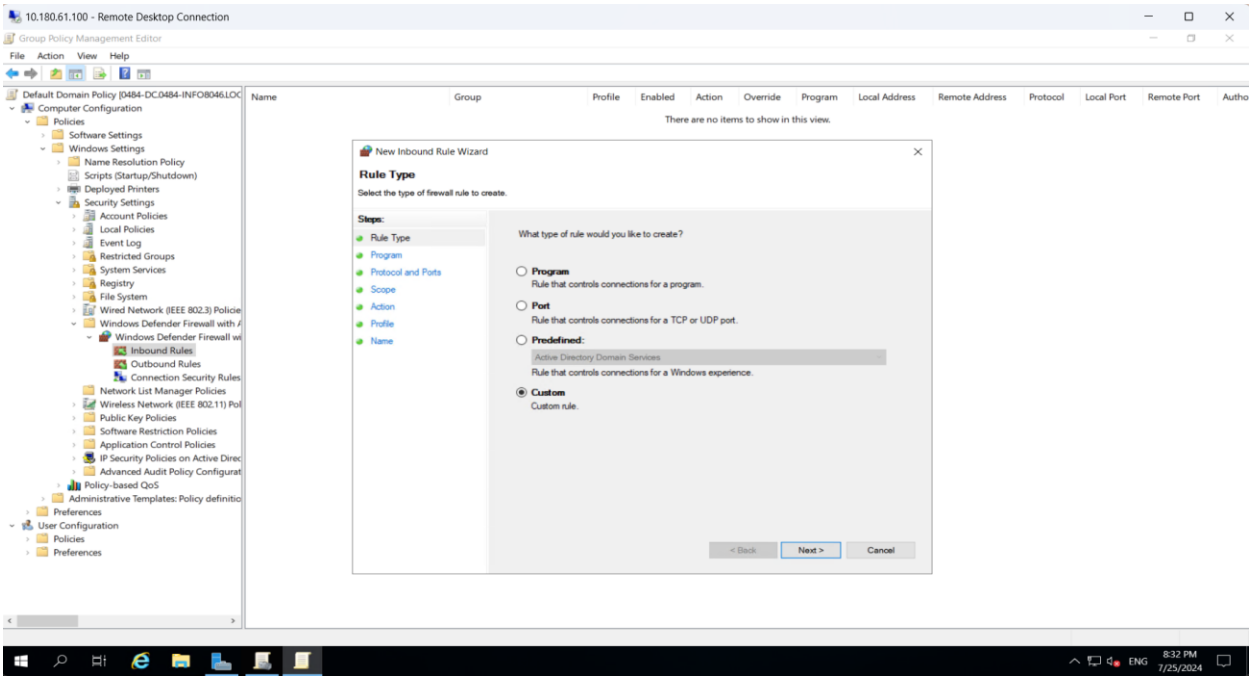

Fig 22: Picture shows creating the New Inbound rule to open the new rule wizard and select the custom type.

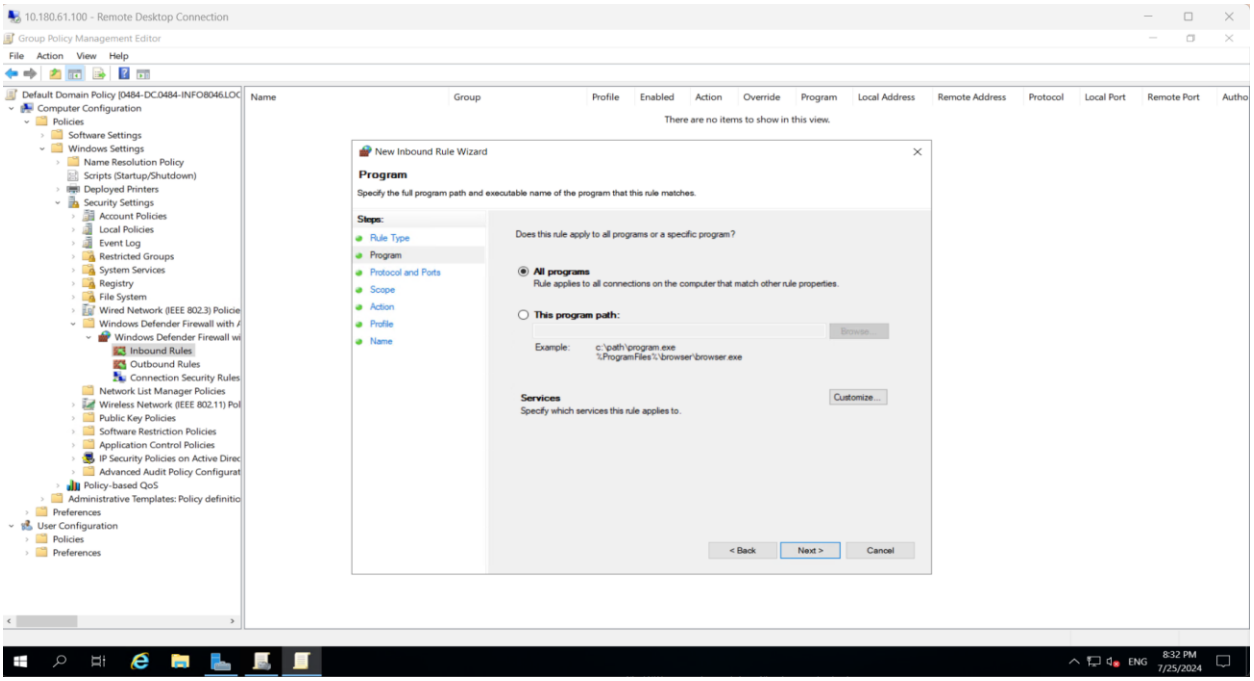

Fig 23: Picture shows All programs that we selected on the programs page.

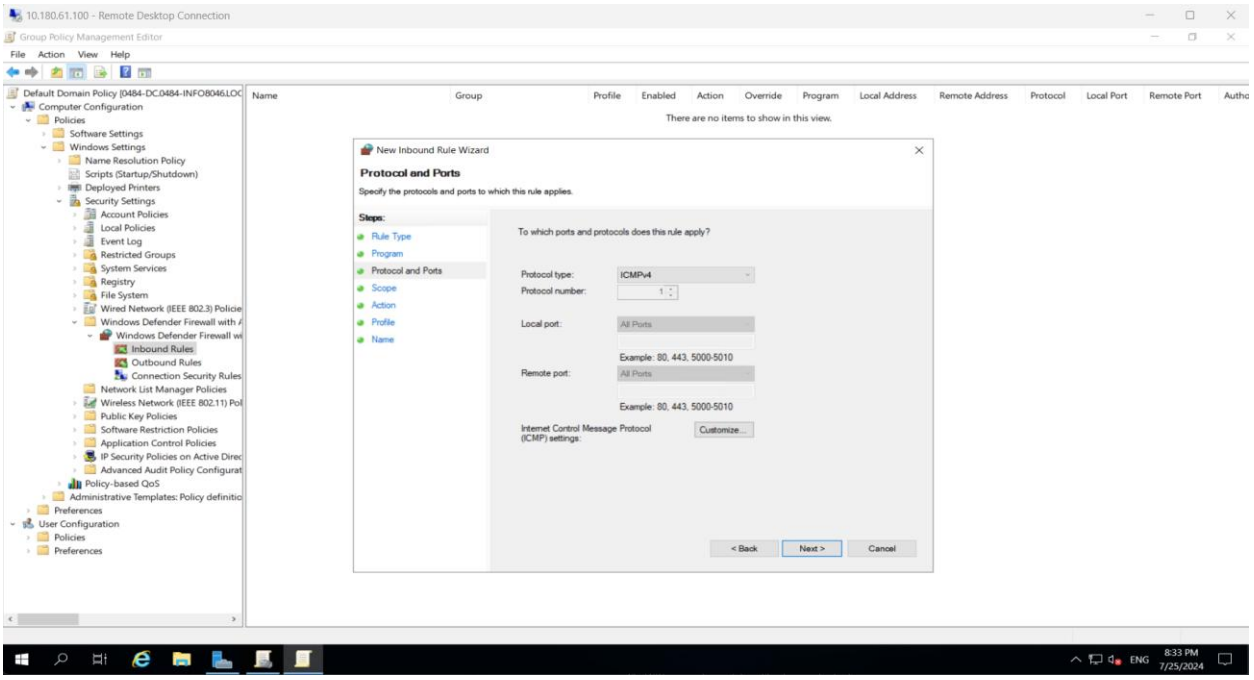

Fig 24: Picture shows ICMPv4 protocol type we selected on the protocol and ports page.

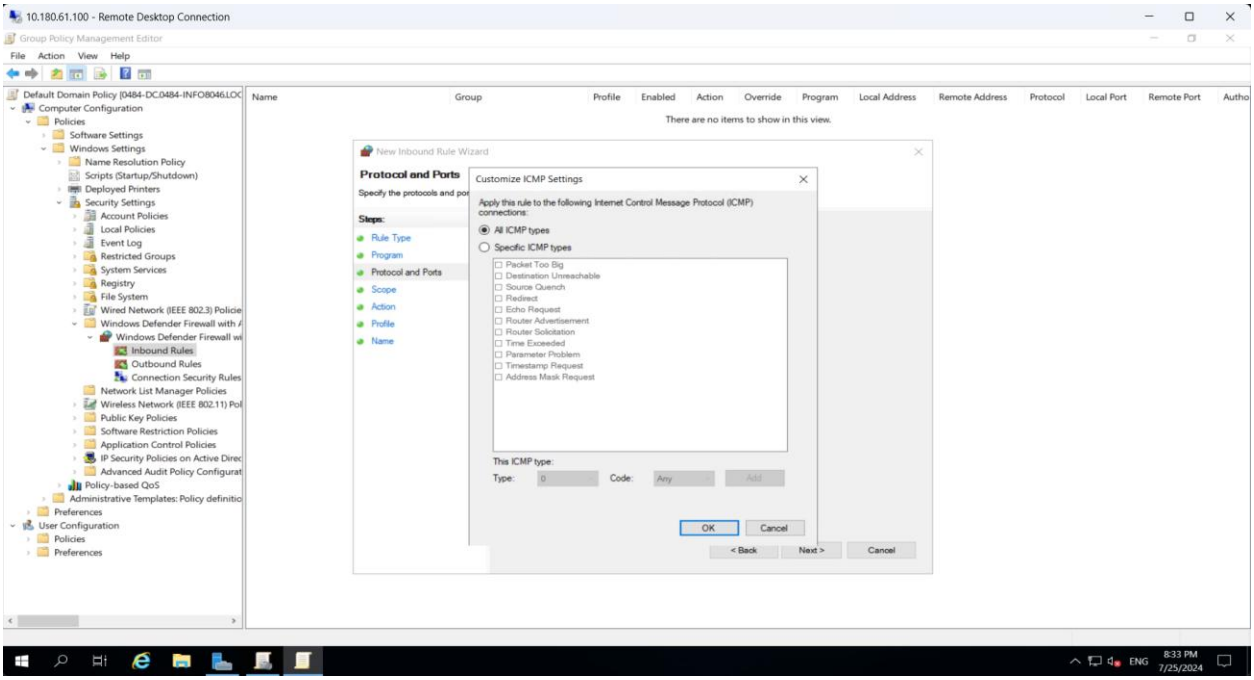

Fig 25: Picture shows select All ICMP types we selected into the customized the setting wizards.

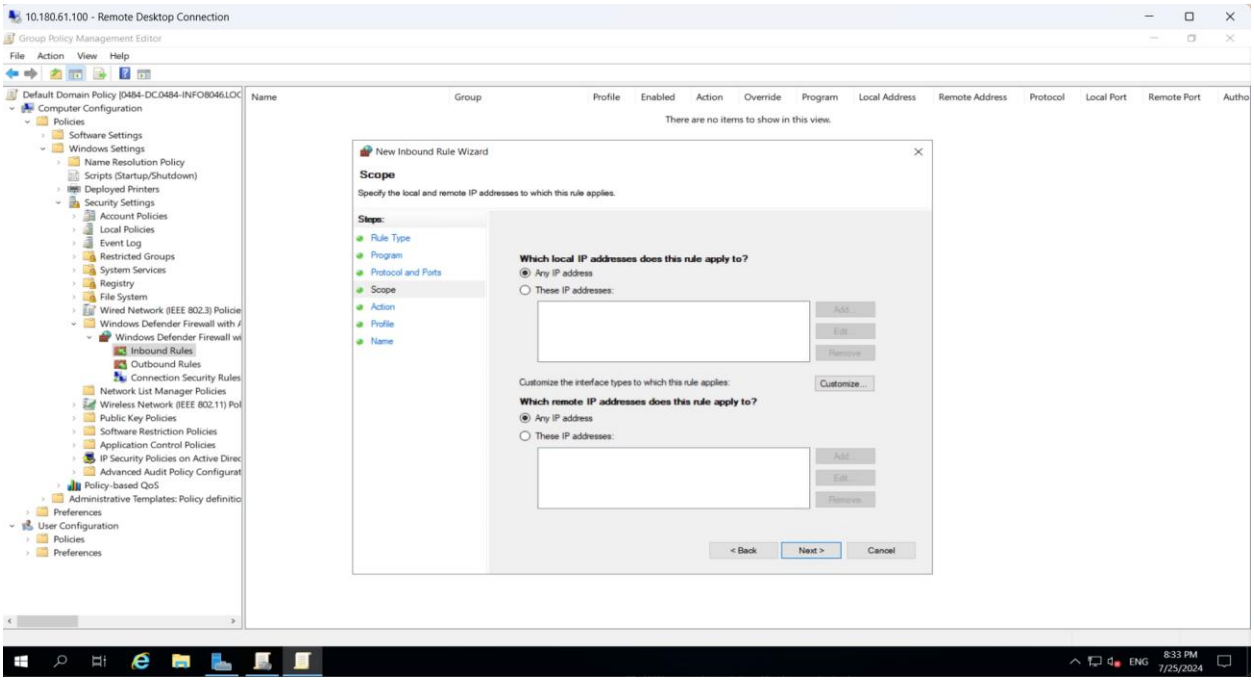

Fig 26: Picture shows default setting into the scope page.

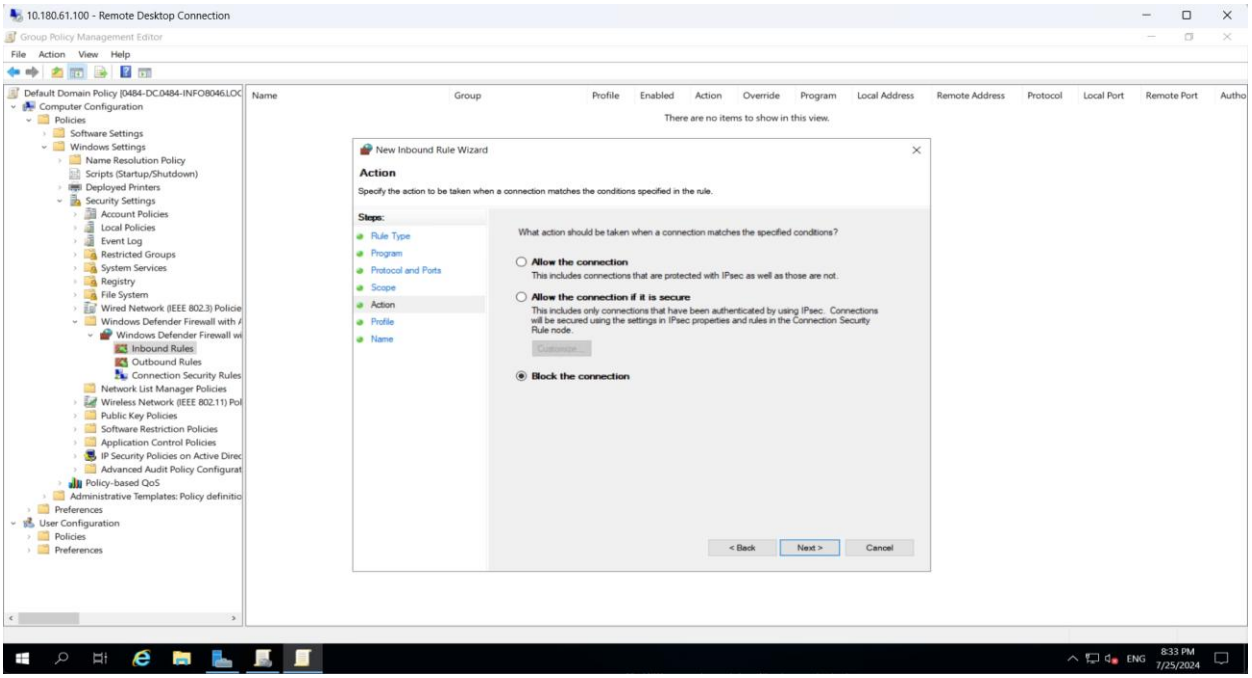

Fig 27: Picture shows selecting the Block the connection into the Action page.

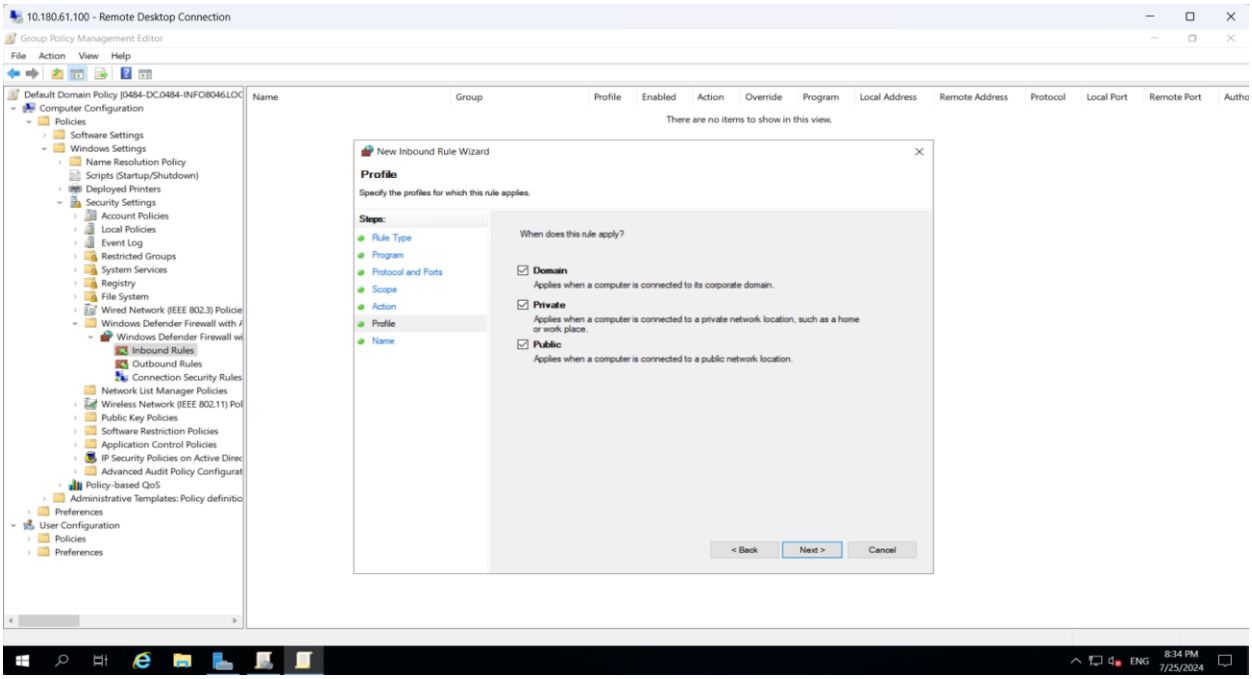

Fig 28: Picture shows accept the defaults onto the profile page.

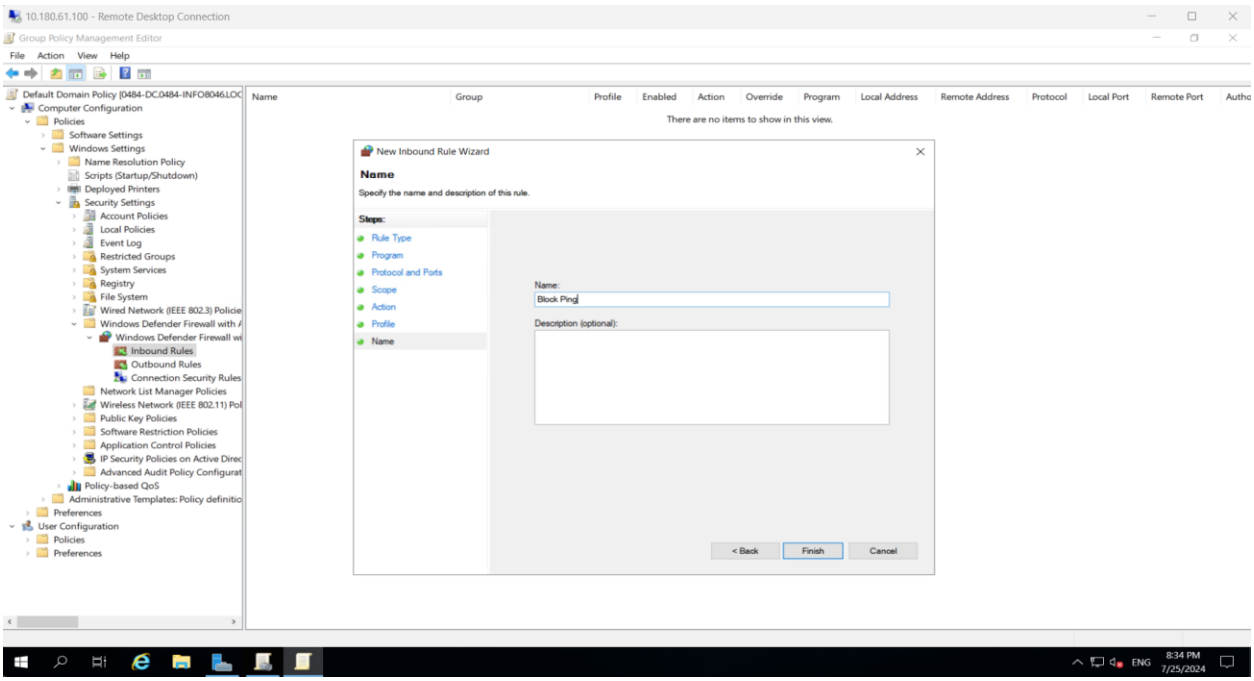

Fig 29: Picture shows given the named by “Block Ping” of the new rule.

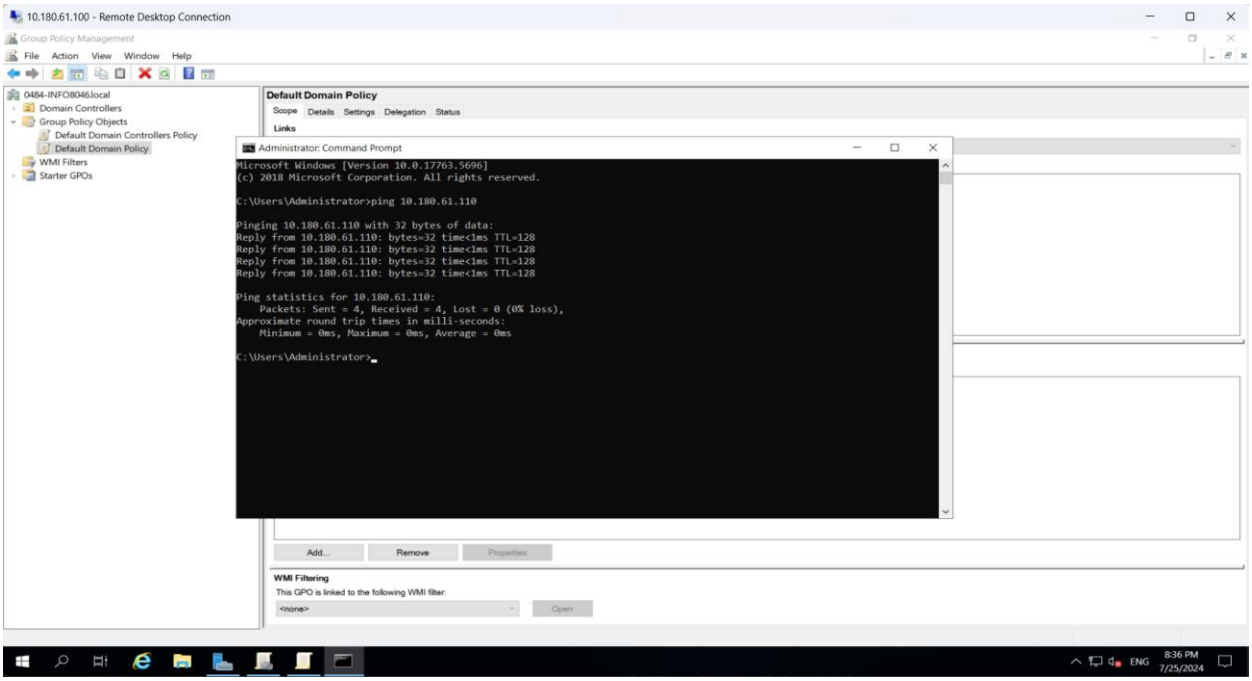

Fig 30: Picture shows pinging from the “Main DC to Testing DC” IP addresses for the checking of pinging because we are not blocking the firewall of “Testing DC machine”.

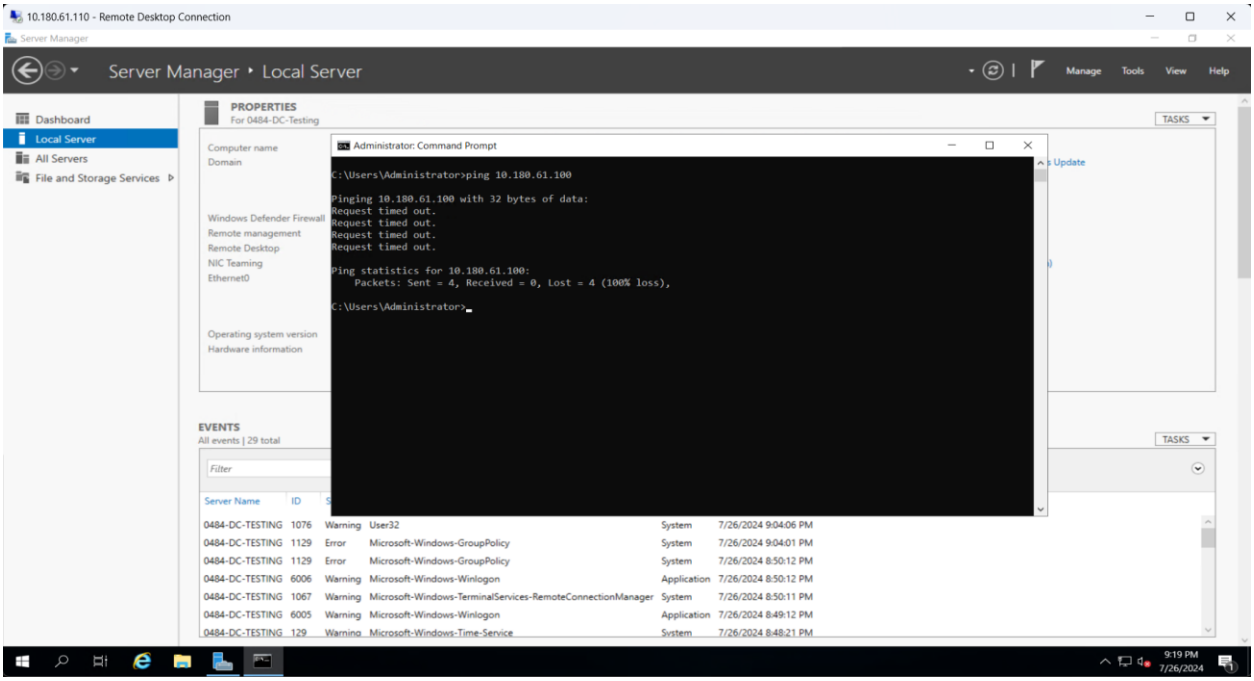

Fig 31: Picture shows pinging the Test DC to main DC which will not be successful because we Block the firewall on the Main DC.

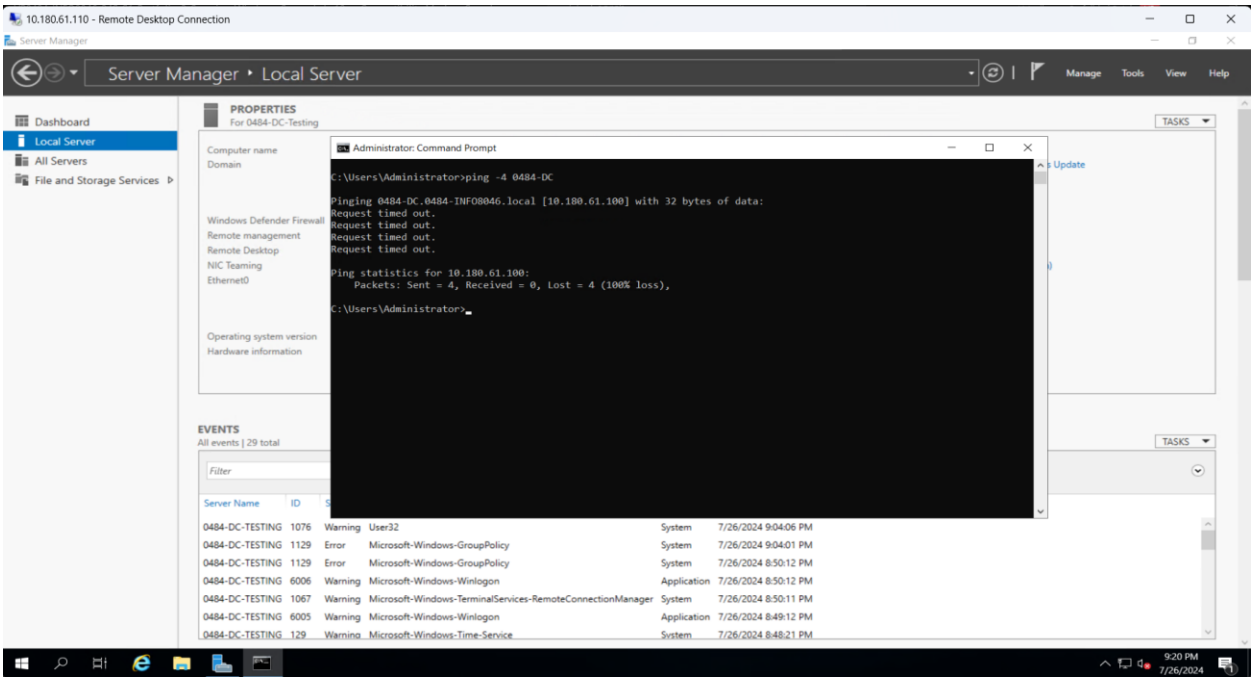

Fig 32: Picture shows pinging the command “ping -4 0484-DC” from Test DC to main DC which will also not be successful because we Block the firewall on the Main DC.

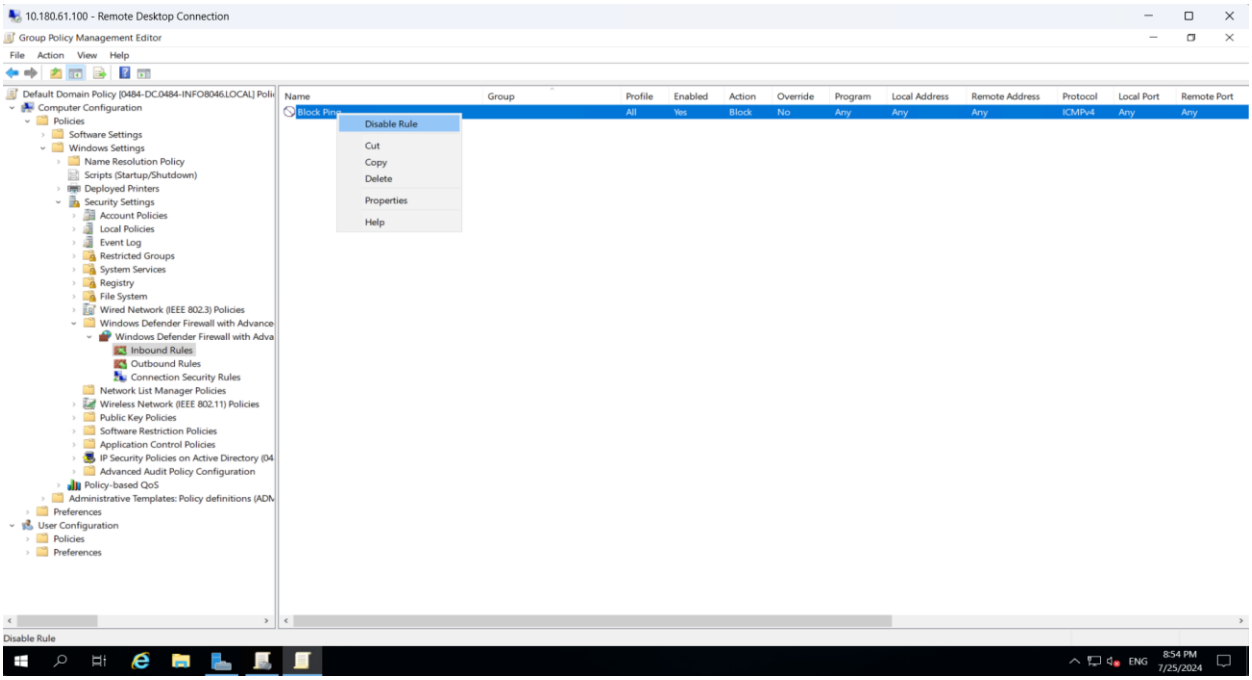

Fig 33: Picture shows disabling the firewall rule Block ping from the Inbound rules.

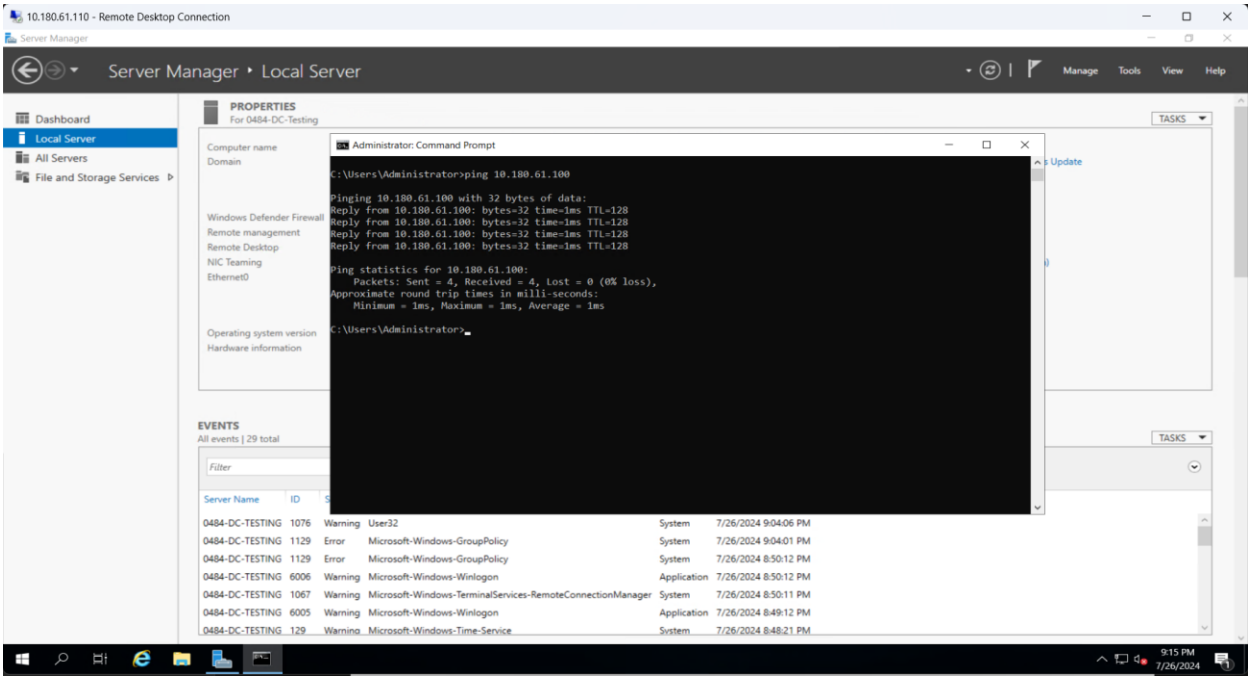

Fig 35: Picture shows after disabling the rules ping will be successful on the Test DC to Main DC.

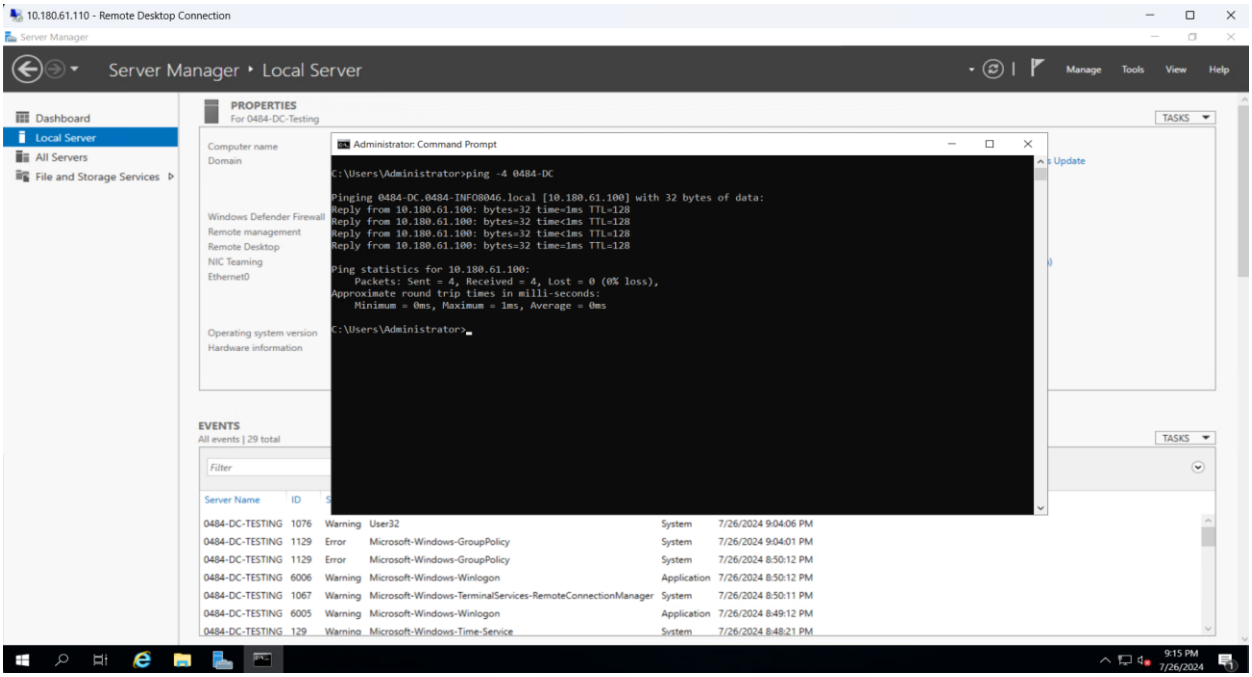

Fig 36: Picture shows pinging the command “ping -4 0484-DC” from Test DC to main DC which will also be successful.

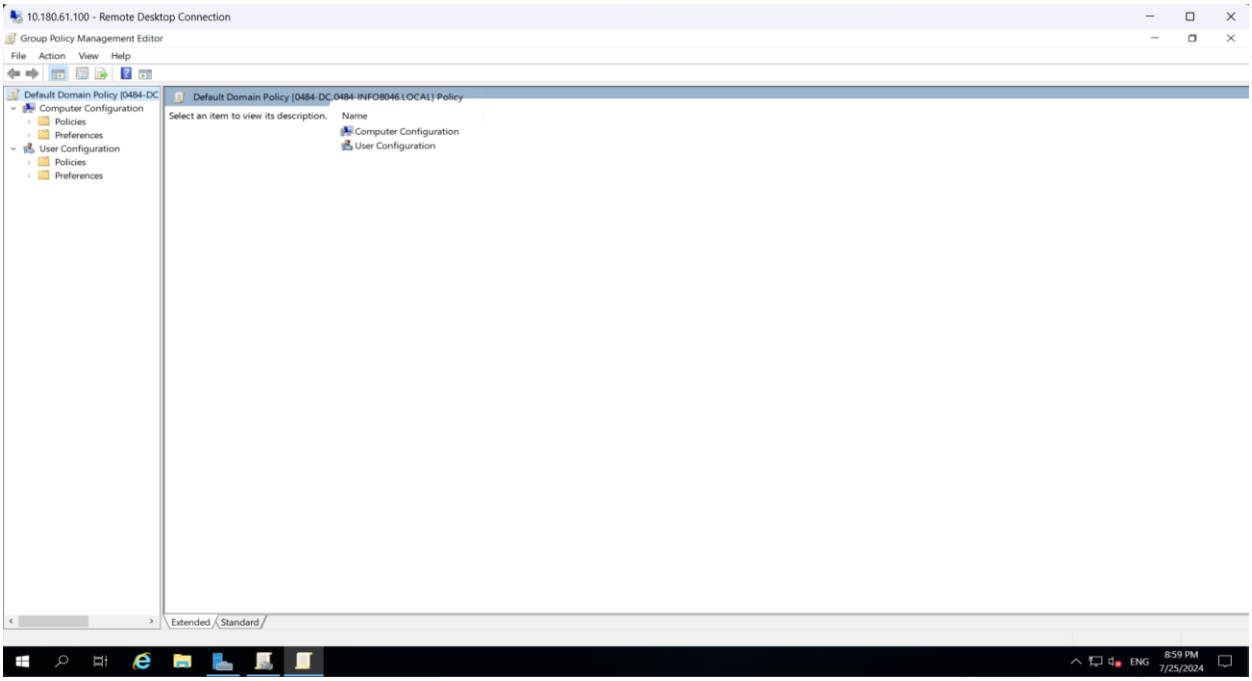

Fig 37: Picture shows open the default domain policy into the Group Policy Management.

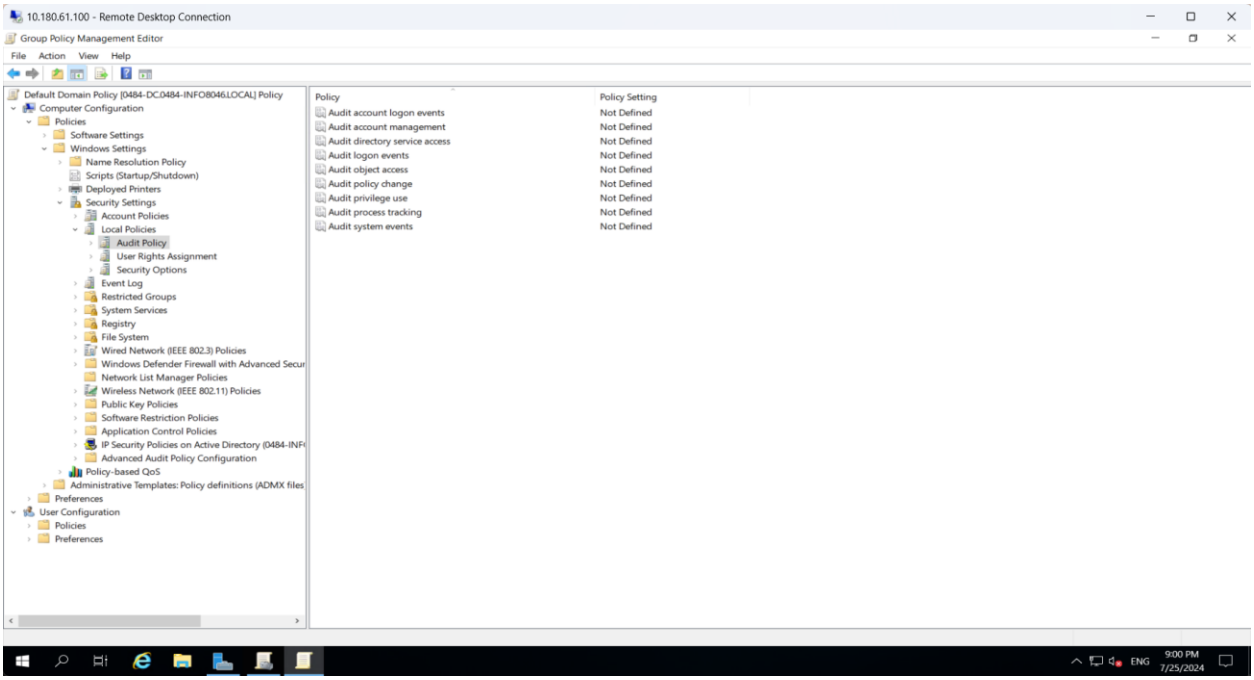

Fig 38: Picture shows navigating the Audit Policy inside the security setting of the domain policies.

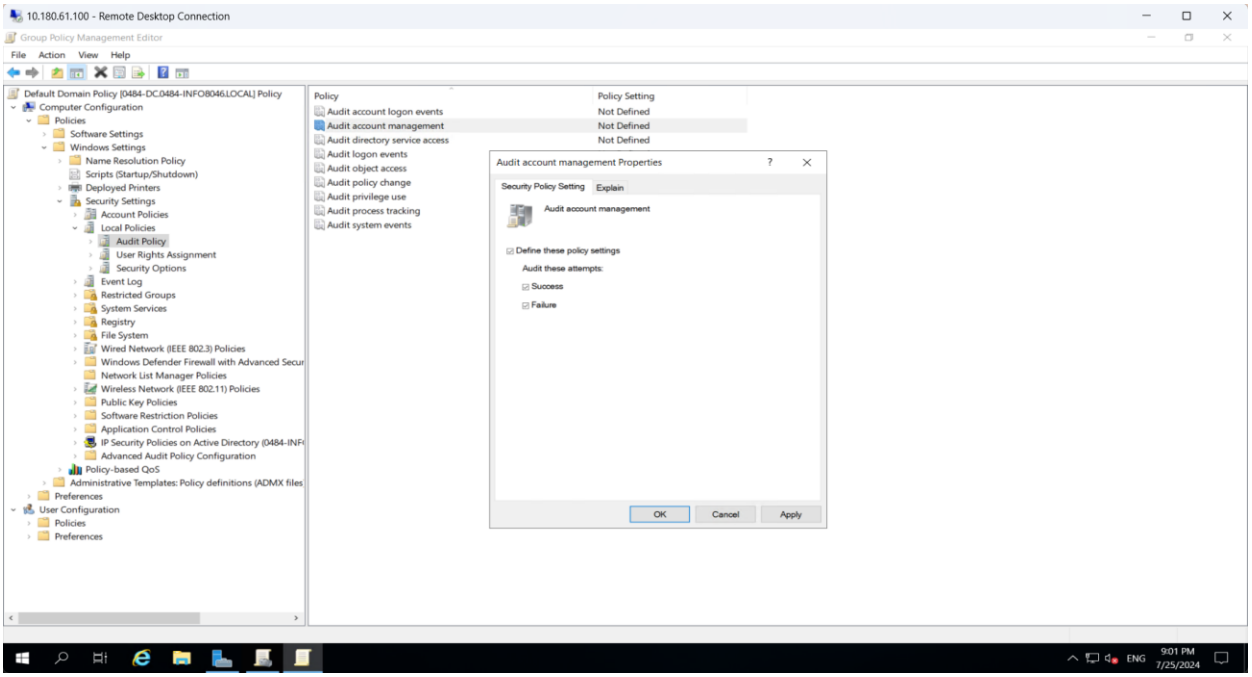

Fig 39: Picture shows selecting one of the policies and check mark the success and failure check boxes into the audit attempts .

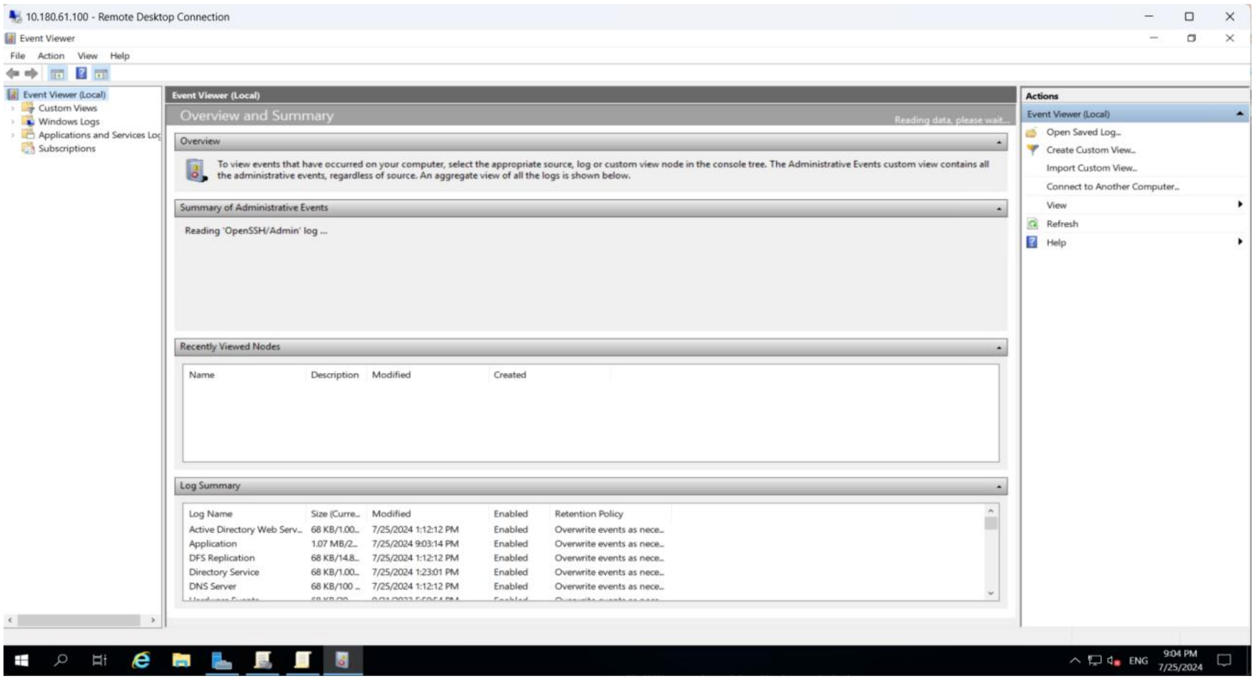

Fig 40: Picture shows open the Event Viewer from the start menu.

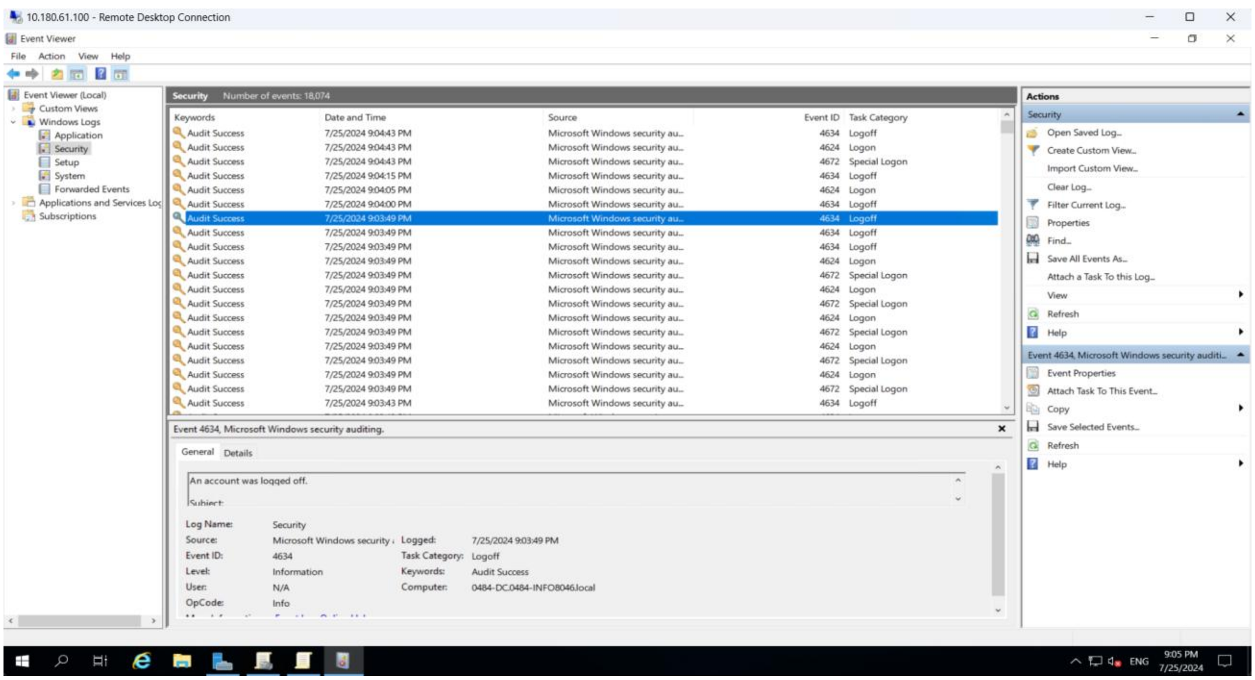

Fig 41: Picture shows expanding the Security windows logs.

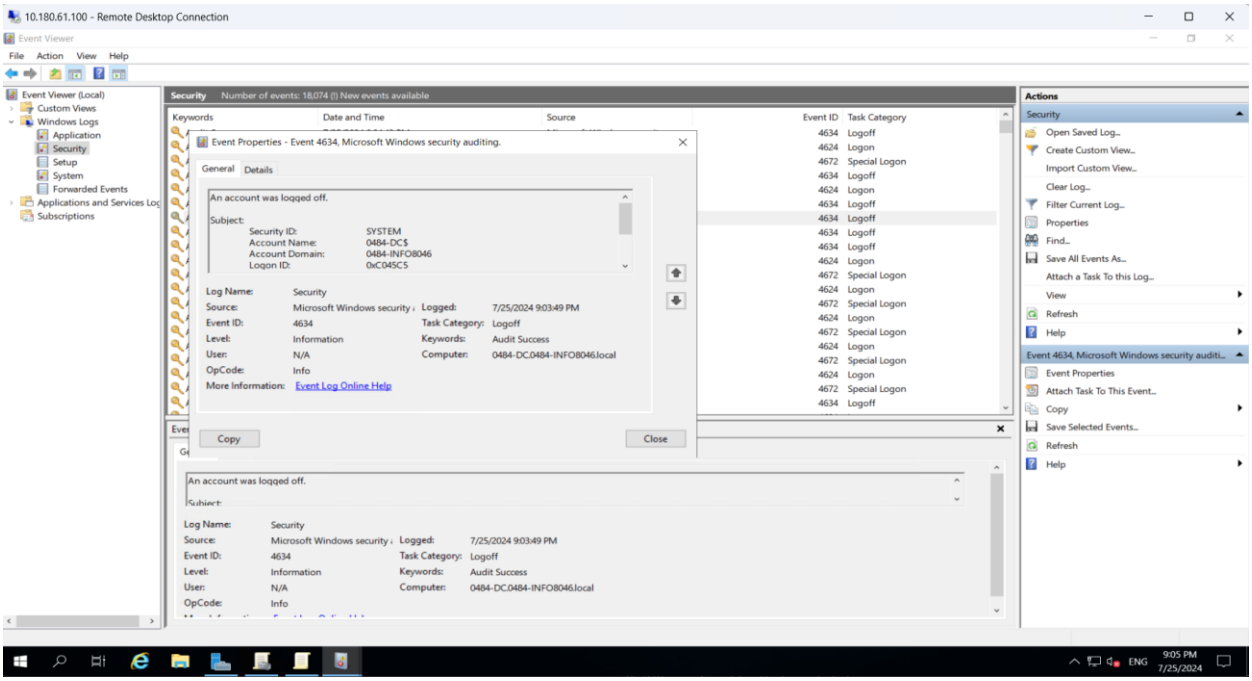

Fig 42: Picture shows reviewing one of the security events into the Event Viewer.

Reflection

The lab exercises associated with the Windows Server security course are very beneficial and important for the real-life implementation of security mechanisms, including EFS, Windows Firewall, as well as setting up the Audit Policies. Interacting with EFS explained how to increase protection of the files and folders by encrypting them, and green colored directory icon illustrated that it is currently encrypted. This exercise highlighted the need to observe data security and how such practices as encryption are flexible and can be passed on to subfolders and files making it comprehensive.

The practical part where I configured the Windows Firewall through GPM to block ICMP traffic highlighted the importance of different measures used in a network to prevent an unauthorized scan of the network. The lessons learnt in developing policies for a firewall and testing of these policies proved useful in explaining the effectiveness of a centralized security policy in a domain. Also, establishing and examining audit policies discussed the importance of monitoring and logging as key elements in ensuring servers' inviolability and tracking possible security threats. All these exercises in aggregate helped to emphasize the need to use various layers of security: cryptography, traffic regulation, and record keeping preventing a threat.

Questions

Exercise 1

1) Did the EFS folder change color? If yes, what color is it?
Ans. Yes, it will change to Green Color

2) Create a new folder under the EFS folder. Is the folder color the same as the parent folder? Why do you think this is?
Ans. Yes, it will be the same color as a parent color because it will inherit the encryption property from the parent folder, and I will try to create the folder also.

3) Create a file under this folder (e.g. text document). Do you notice anything different about the file? Zoom in on the file and note what the difference is.
Ans. The file creating in this folder which will also in Green Color and encrypted

Exercise 3

1) Which of these policies do you need to configure when you need to see when someone uses privileges to access, copy, distribute, modify, or delete files on file servers?
Ans. Audit Object Access

2) Which policy can you configure to detect all unauthorized attempts to log in to your domain?
Ans. Audit Logon Events

3) Which policy setting allows you to audit events generated by authorization policy changes, such as the Encrypted File System (EFS) policy?
Ans. Audit Policy Change

4) Why is it good practice to monitor everyone instead of user(s) or group(s) when auditing?
Ans. Monitoring everybody allows the coverage of all the spheres of protection and gives feedback on the unauthorized or malicious actions of any user or group to improve the safety condition.