jamk

AD hardening- Lab 1

Group 4

Nguyen Ngo - AE8880
Dung Doan - AA7785
Syed Fawaz - AD9946
Jasper (Franciscus) van de Klundert - AG9056
Sanka De Silva - AC4892

Exercise Lab 2

Data Security Control

10/02/2025

Bachelor’s Program of Information and Communication Technology

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Contents

1 Introduction

The purpose of this first laboratory exercise is to harden the Active Directory (AD) environment. The group can choose their preferred hardening guide, but since Microsoft products are being hardened, it might give some direction. Using the chosen guide, you should harden the following:

- Windows Server (SRV01, refer to its specific guide)
- Windows AD hardening (DC01)
- Group policy hardening (DC01)
- To verify the AD hardening, use MS BPA (available on all Windows servers)

The hardening process must be documented, explaining what is done and why. It is probably sensible to first run the analyzer, record the results, then harden, run the analyzer again, and see if any changes were made.

2-2-2025. Today virtual learning environments doesn't respond to keyboard.
In the first lab work of the "Hardening" course module, the aim is to harden our virtual environment's file server (SRV01) and Active Directory (DC01) (Figure 0). In the process of hardening the Active Directory, we also hardened the Group Policies. For hardening the file server, specific instructions were provided, but we chose our own guide for hardening the Active Directory. Our group selected the Center for Internet Security (CIS) Benchmarks guide found in the course materials, and we also reviewed other guides, such as Microsoft's own best practices guidelines. The aforementioned guide is very extensive, so we did not implement everything mentioned there; instead, we chose what we considered important hardenings to implement.

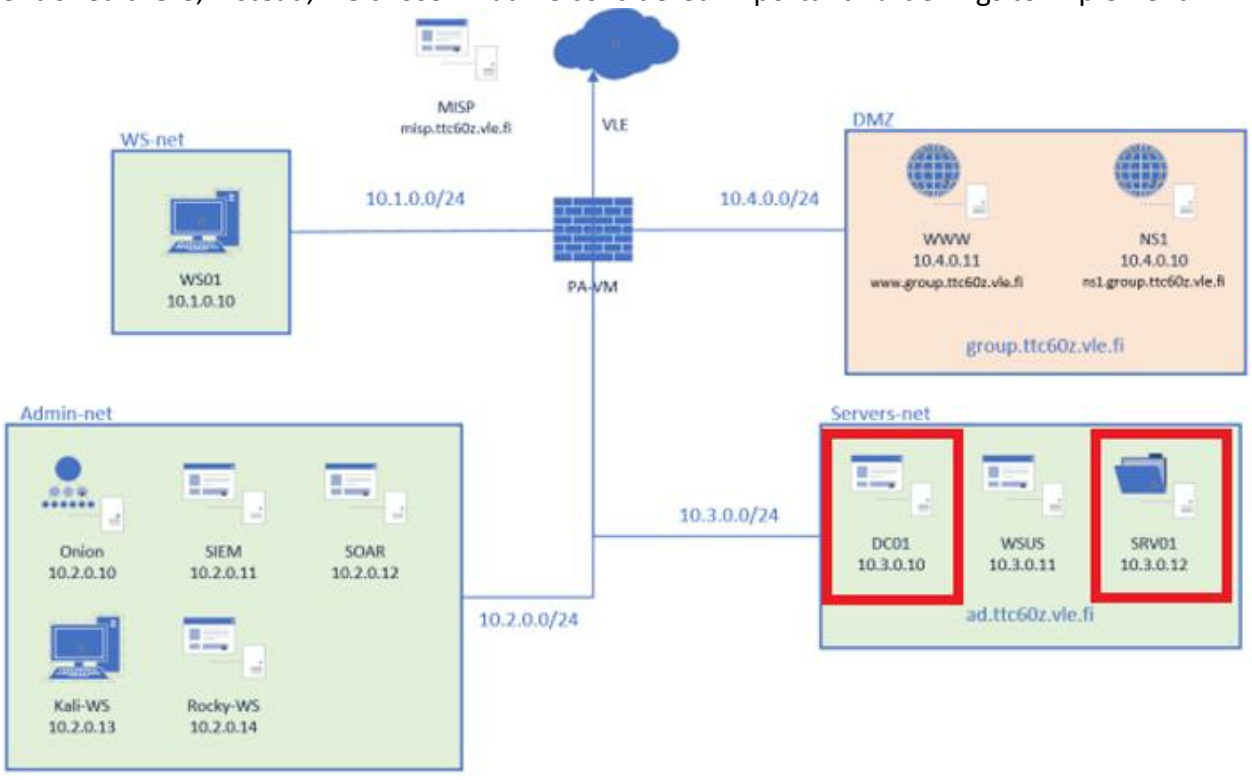


Figure 0. Server

1 Theory of the lab

Hardening refers to enhancing the security in information systems, network devices, servers, and software. Hardening can be done, for example, by removing unnecessary and outdated applications, software, and roles with the goal of reducing the attack surface area and thereby decreasing the opportunities that potential attackers can use to enter the system or damage it. (Schrader, D. 2023)

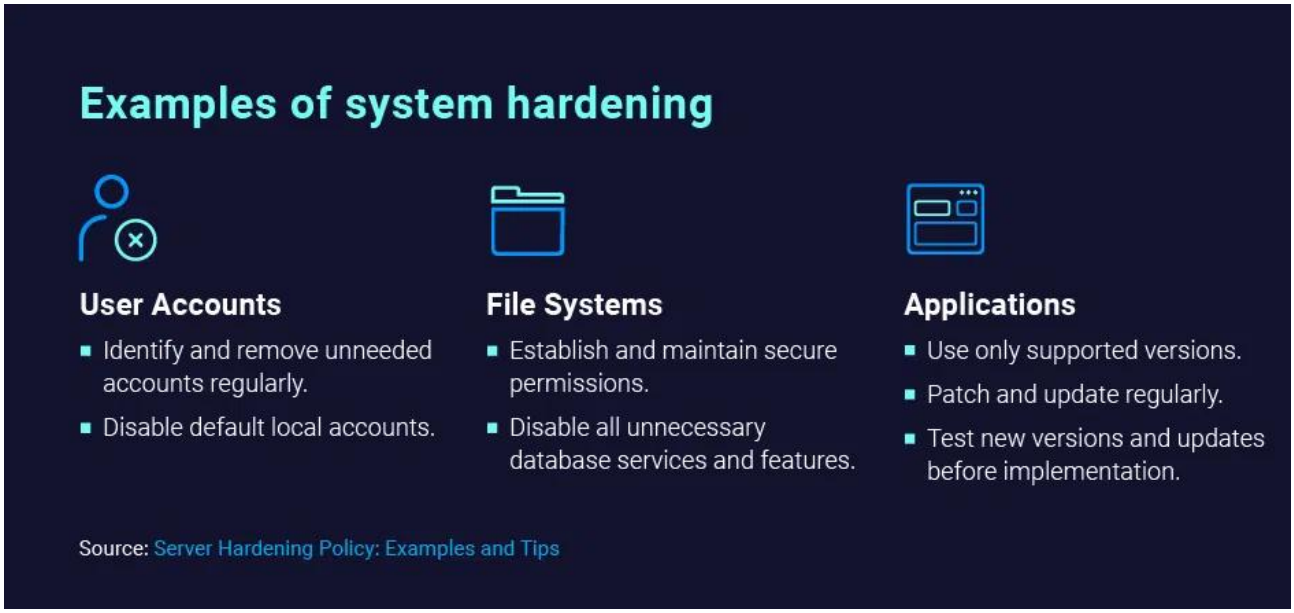


Figure 1. Examples of Hardening

Hardening also includes managing user rights. User rights can be managed, for example, using the Principle of Least Privilege. This means that users, applications, and processes are only given the rights that are necessary for them to perform their tasks. This aims to reduce the risk of unauthorized access and erroneous actions that could lead to security threats or breaches. For example, a warehouse worker does not need access to manage the company's website, nor does a salesperson necessarily need to make changes to the computer's firewall settings. (Schrader, D. 2023)

1.1 FileServer

A file server is a server within a network that provides a centralized location for users and other system components to store, manage, and share files. This server can contain documents, soft-

ware, images, backups, and other types of data, and it allows access to these files from various devices and locations. The key functions of a file server include the secure storage of files, backup, sharing, and management of access rights. Managing access rights helps determine who can read, modify, or delete specific files. This is a crucial part of information security and hardening. (Wright, G. 2023)

The file server we use operates on Windows Server 2019 and utilizes the SMB (Server Message Block) protocol, which ensures fast and secure file sharing. There are three versions of SMB: SMB1, SMB2, and SMB3. As of 2024, SMB1 is no longer considered secure and should not be used (Copilot).

This comprehensive approach to managing a file server ensures that organizational data is secure, accessible, and efficiently managed.

1.2 Active Directory

Active Directory (AD) is a database and service suite that contains information about users, computers, and network resources. AD connects users to the necessary network resources to accomplish their tasks. It operates on Windows Server and allows system administrators to manage access rights and the use of network resources. (Simister, A. 2024)

The database holds critical information about your environment, such as which users and computers are part of it, as well as rules about who is allowed to do what. The service monitors the environment and ensures authentication, verifying that each person is who they claim to be and that they have access only to the information they are authorized to access. Active Directory enhances an organization's security and allows administrators and users to operate easily and securely. System administrators can manage users and access rights across the organization, as well as manage computer and user configurations through AD Group Policy.

The most important Active Directory service is Active Directory Domain Services (AD DS), which is part of the Windows Server operating system. Once AD DS is installed on a server, it becomes a domain controller (DC). This server stores the entire AD database. An organization typically has several DCs. AD DS is based on various protocols and standards, such as LDAP, Kerberos, and DNS (Simister, A. 2024).

Active Directory plays a crucial role in ensuring IT infrastructure is secure, structured, and efficiently managed, contributing significantly to organizational control and security strategies.

1.3 Other Applications

1. **Account Lockout Policies** define how failed login attempts are handled in AD; for example, an account is locked after three attempts and the lock lasts for a certain period. Configuration must consider the risk of potential security threats (Brute-force attack) and at the same time the usability of the function for the users themselves. (Allen R., 2023)
2. **Strong Password Policies** configuration in Windows AD can protect user accounts and other resources from hackers' intrusion attempts, such as brute force attacks and guessing of easy passwords. The CIS STIG Benchmark document has requirements for password length, complexity, and change intervals. For example, a password must be at least 14 characters long, include numbers and special characters, the minimum password history is 24 previous passwords (cannot set a password previously used), the maximum password age is 60 days, and the minimum age (when it can be changed again) is at least 1 day. (CIS. 2019. Section 1.1 Password Policy)
3. **LAN Manager Hash (LM Hash)** is an outdated hashing algorithm that was used in older Windows operating systems for storing passwords. LM Hash is known for its vulnerabilities; it simplifies passwords by converting them into uppercase and splitting them into two 7-character blocks, each of which is hashed separately. This makes it particularly susceptible to brute-force attacks, as the simplicity and predictable structure lower the complexity needed to crack the hashes. Modern systems no longer use LM Hash due to these security flaws (Lark, 2024).
4. **SMB (Server Message Block) Signin**g is a security feature that enhances the integrity of SMB protocol traffic by adding digital signatures to packets. This verification prevents unauthorized interception and modification of data during transit, safeguarding against security threats like man-in-the-middle and replay attacks. SMB Signing ensures that data remains secure and unaltered, reinforcing network communications against potential intrusions by hackers((Microsoft network server: Digitally sign communications (always). 2023).
5. **LDAP (Lightweight Directory Access Protocol)** is a protocol that facilitates the use of directory and database services over a network. It allows for retrieving, updating, and deleting data from directories such as Active Directory. LDAP serves as an interface to Active Directory, enabling the retrieval and modification of its information. LDAP Access Control is used to set restrictions for LDAP users and defines how it can be accessed, ensuring that only authorized individuals and applications can utilize Active Directory (GeeksforGeeks, 2019).
6. **Kerberos** is a protocol utilized in Active Directory for user network authentication, offering a secure means of verifying users without requiring password input through a ticketing system. Upon authentication, users are issued AES-encrypted tickets by the Key Distribution Center (KDC), which allow them access to network services without repeated logins. Best practices in a Kerberos system recommend limiting the validity of tickets to 10 hours to reduce the risk of misuse, employing strong AES encryption to ensure security, and maintaining logs of Kerberos authentications to facilitate the detection of unauthorized access attempts. This comprehensive approach helps in enhancing the overall security framework by preventing potential breaches and ensuring that user credentials are robustly protected (Loshin, P. 2021).
7. **The Microsoft Best Practices Analyzer (BPA)** is a tool integrated into several Microsoft products like Windows Server and SQL Server. It scans configurations and settings of these products, comparing them to industry standards and Microsoft's best practices. BPA produces a report highlighting deviations or violations from these best practices, detailing the severity, explanation, and resolution for each identified issue, thereby helping to improve system security and functionality (Rendell, D. 2024).

2 Working Progress

2.1 FileServer Hardening

The first target for hardening in our environment, found on Servers-Net, was the SRV01 server, which is intended for file server use. We began by removing all unnecessary components from the server to reduce the attack surface. We were able to remove unnecessary roles and features from the upper right corner under "Manage" and "Remove Roles and Features." (Figure 2.)

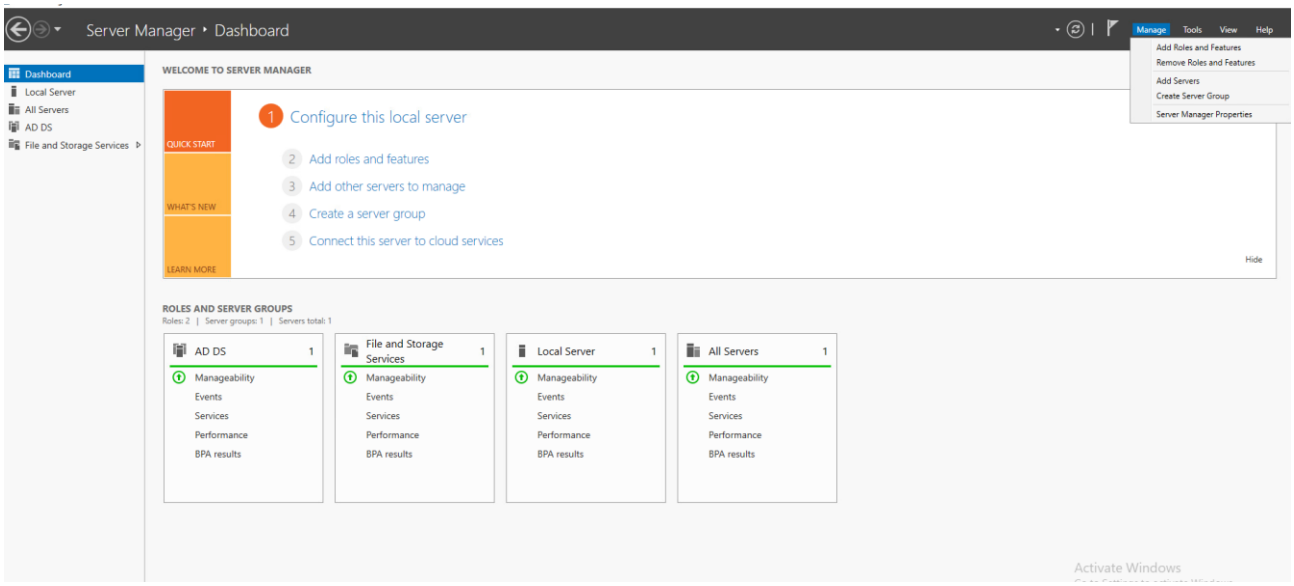


Figure 2. Removing Roles and Features

Then, we clicked the "Next" button in the "Server Selection" section and moved to the "Server Roles" section. In the server roles section, we removed all roles except for File and Storage Services, and then pressed the "Next" button. (Figure 3.)

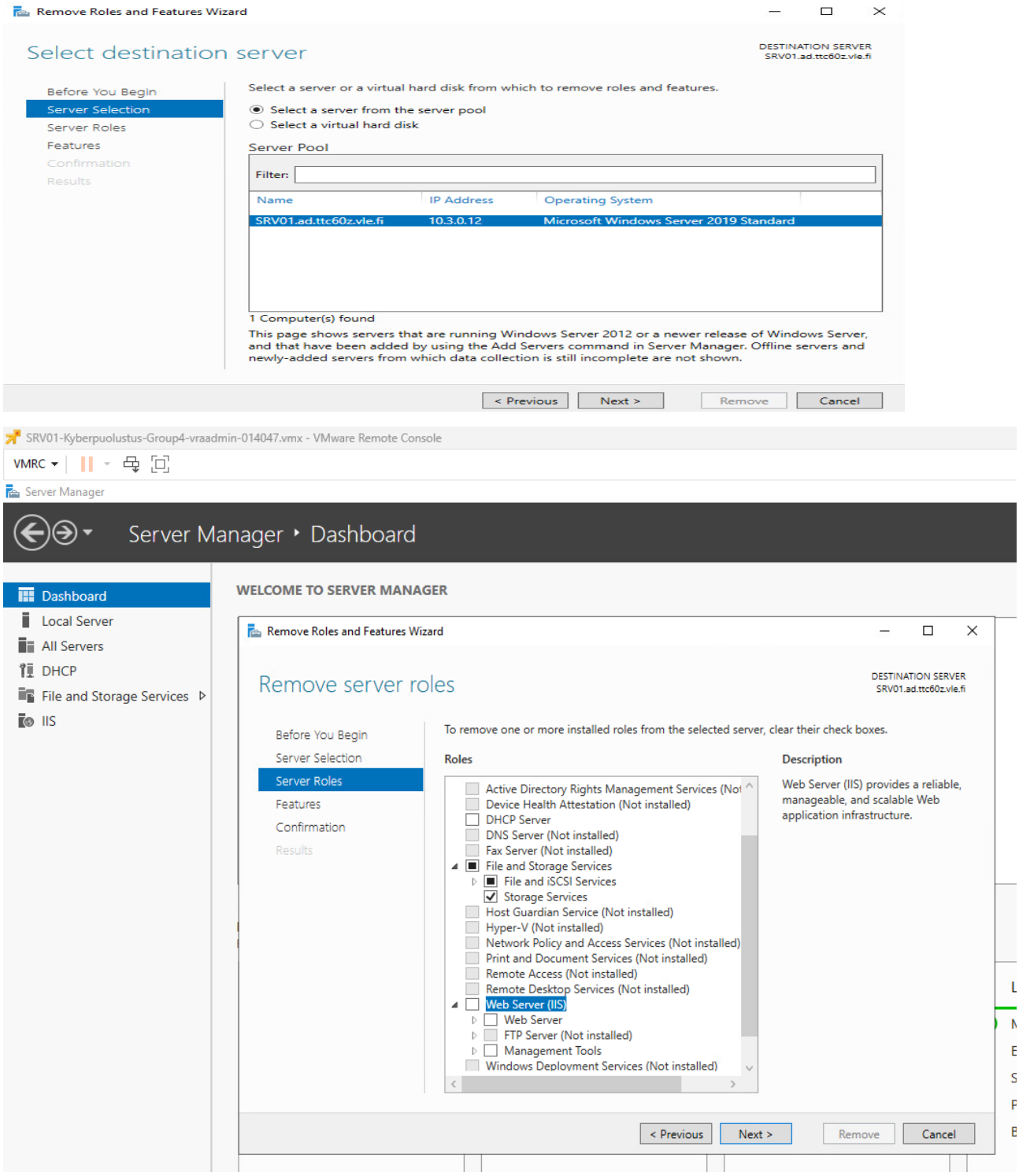


Figure 3. Server Roles

On the Features tab, we deselected all features except for .NET Framework 4.7 features, Group Policy Management, Windows PowerShell, and Remote Server Administration Tool. Others can be added or removed later as needed. (Figure 4.)

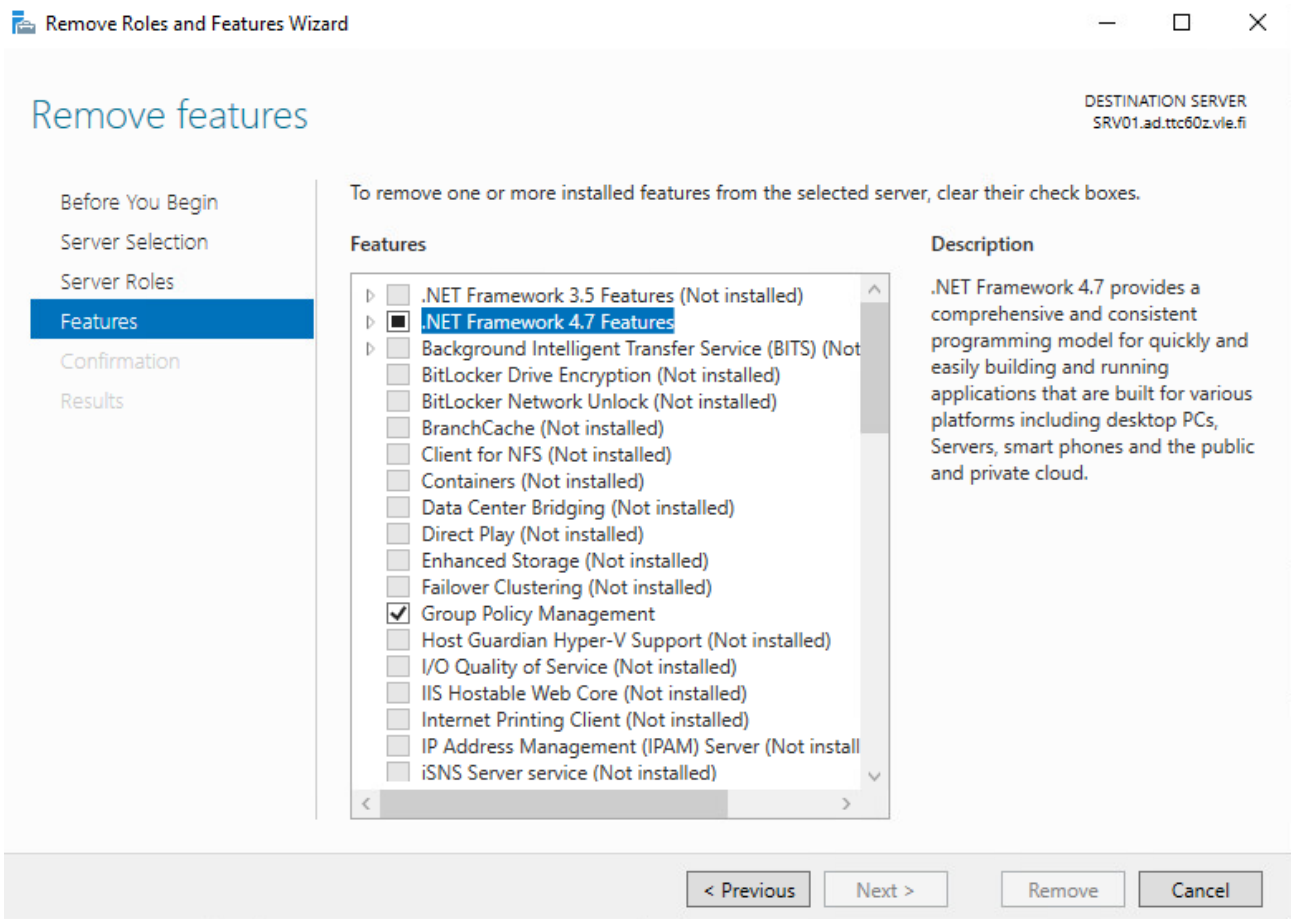
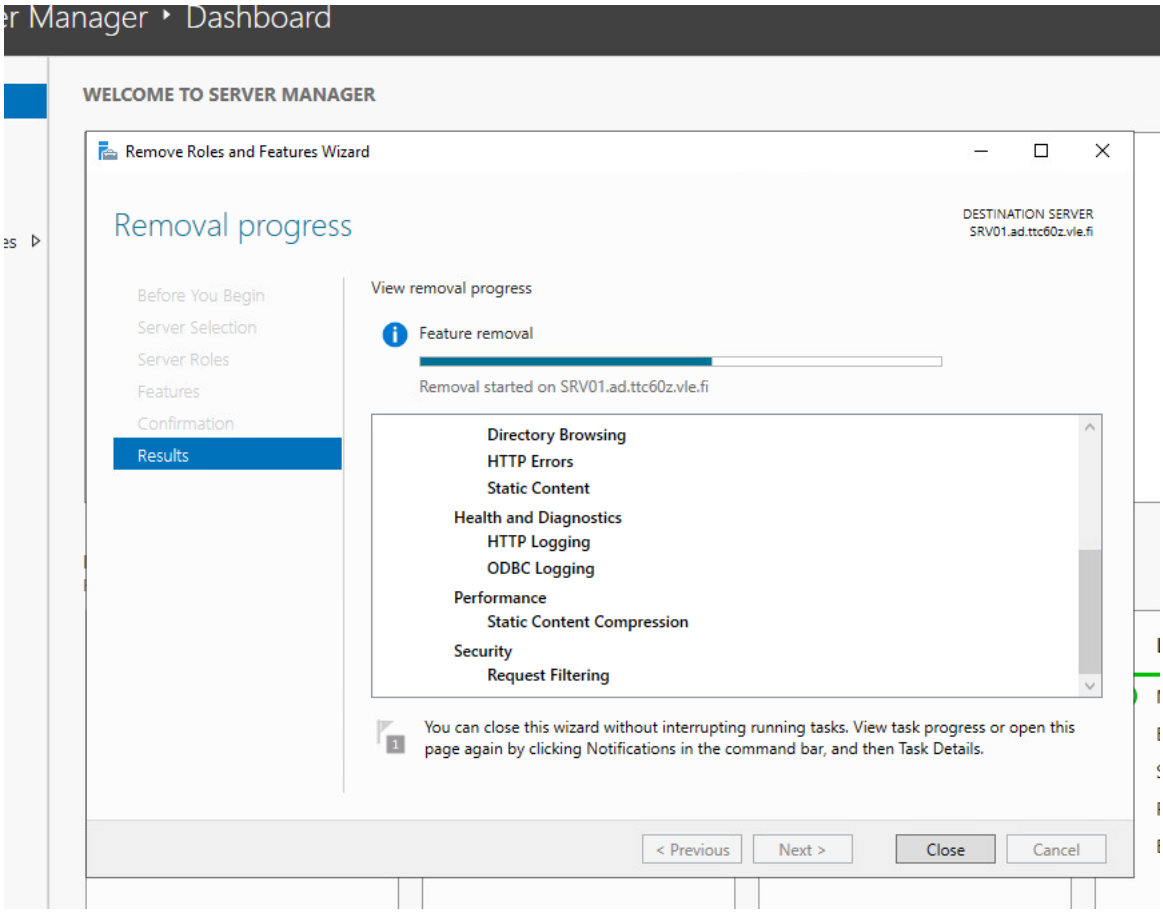


Figure 4. Features

Following that, we proceeded to the Confirmation screen by clicking the "Next" button, where we selected "Restart the destination server automatically if required," and then moved forward once

again. We then installed the appropriate roles and functionalities on the server.



We chose "Add Roles and Features" from the "Manage" menu in the upper right corner (Figure 5).

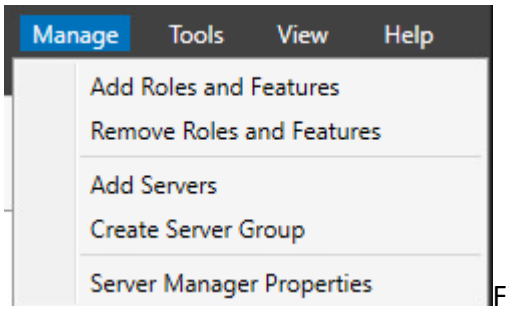
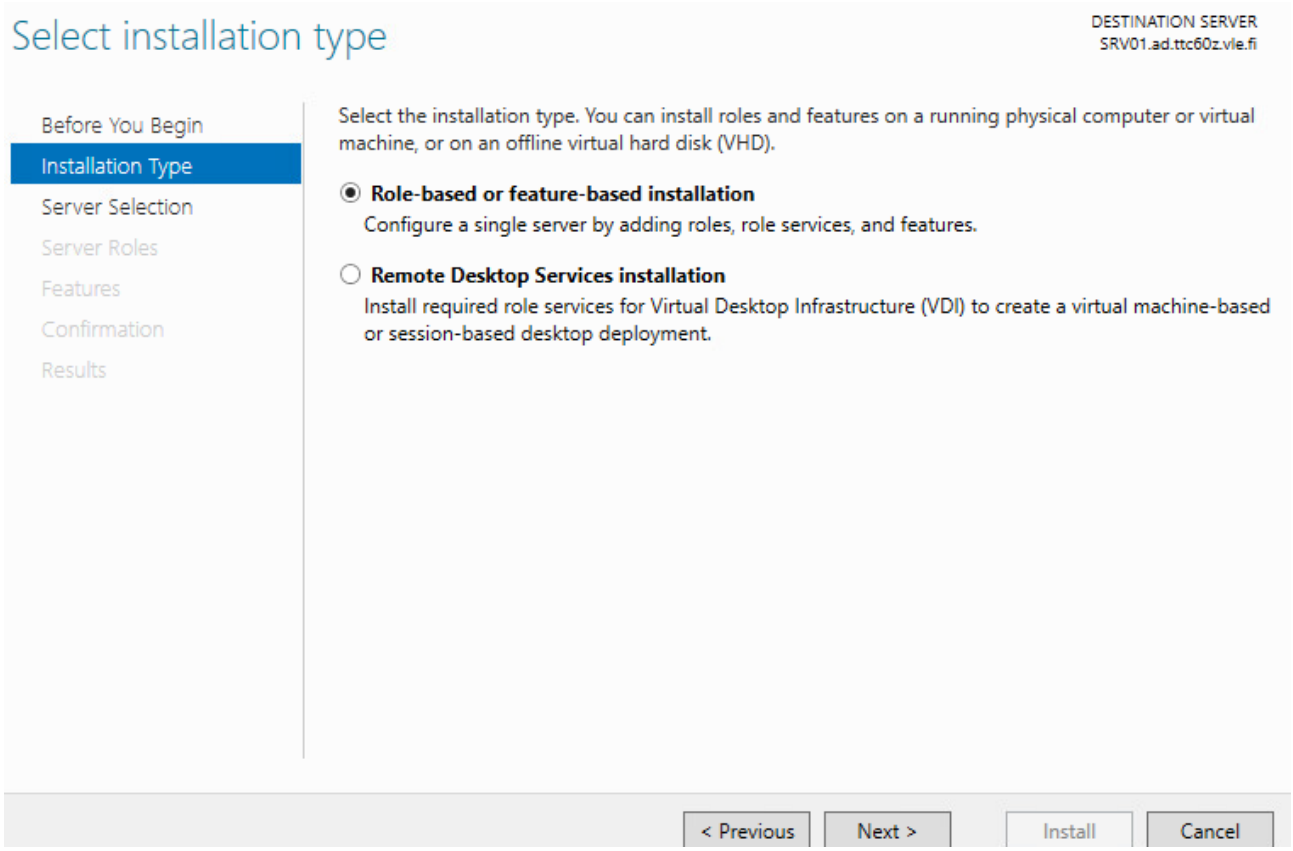


Figure 5. Add Roles and Features

In the Installation Type section, we selected the top option and moved to the next point. In the Server Selection, we once again chose our server, SRV01, which is the only option available. (Figure 6.)



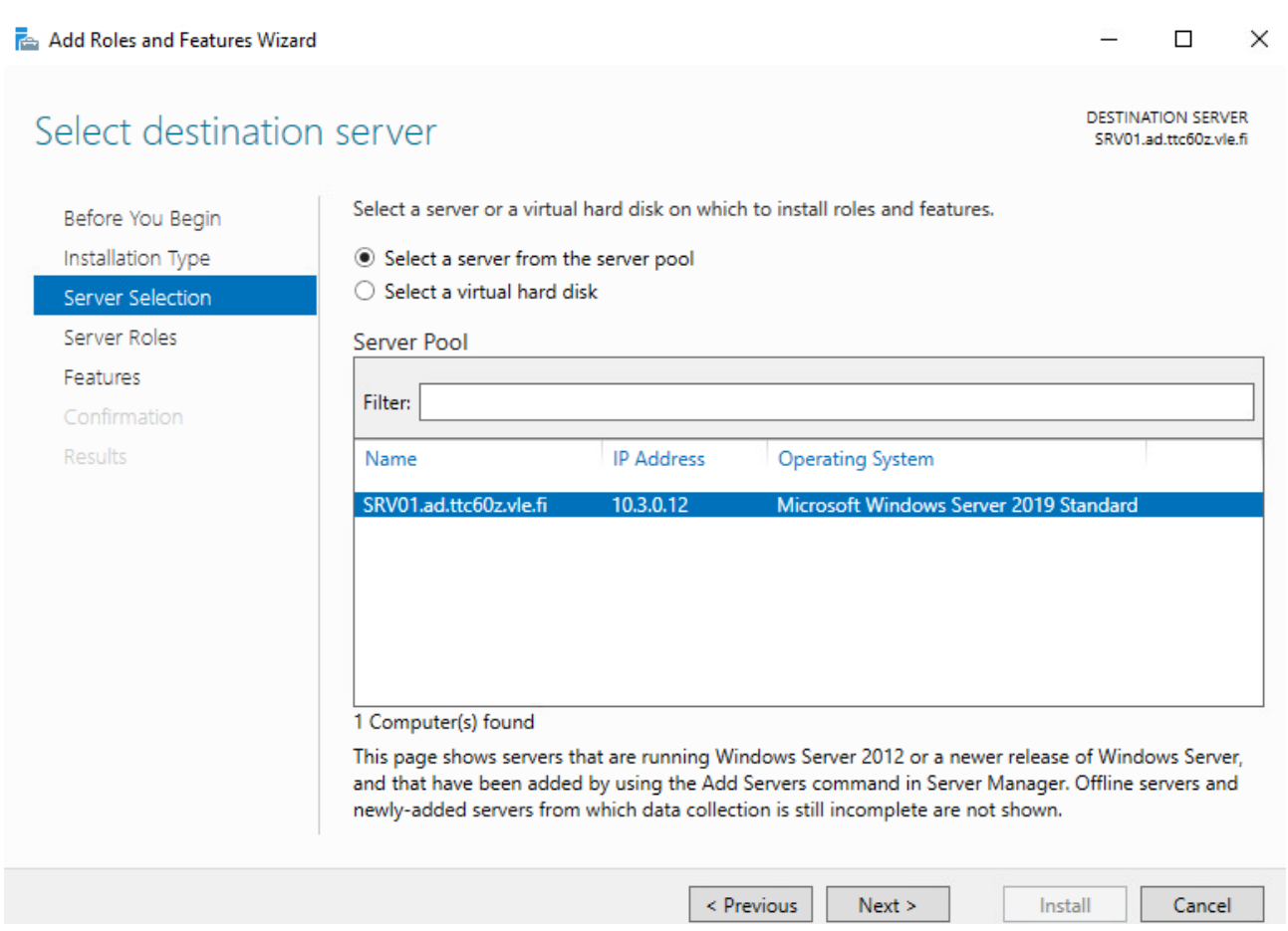


Figure 6. Installation Type and Server Selection

Next, we selected the roles to be installed. Following the instructions, we chose Storage Services under the File and Storage Services category, and File Server under the File Server and iSCSI services category. Figure 7 shows the selected roles already installed. (Figure 7.)

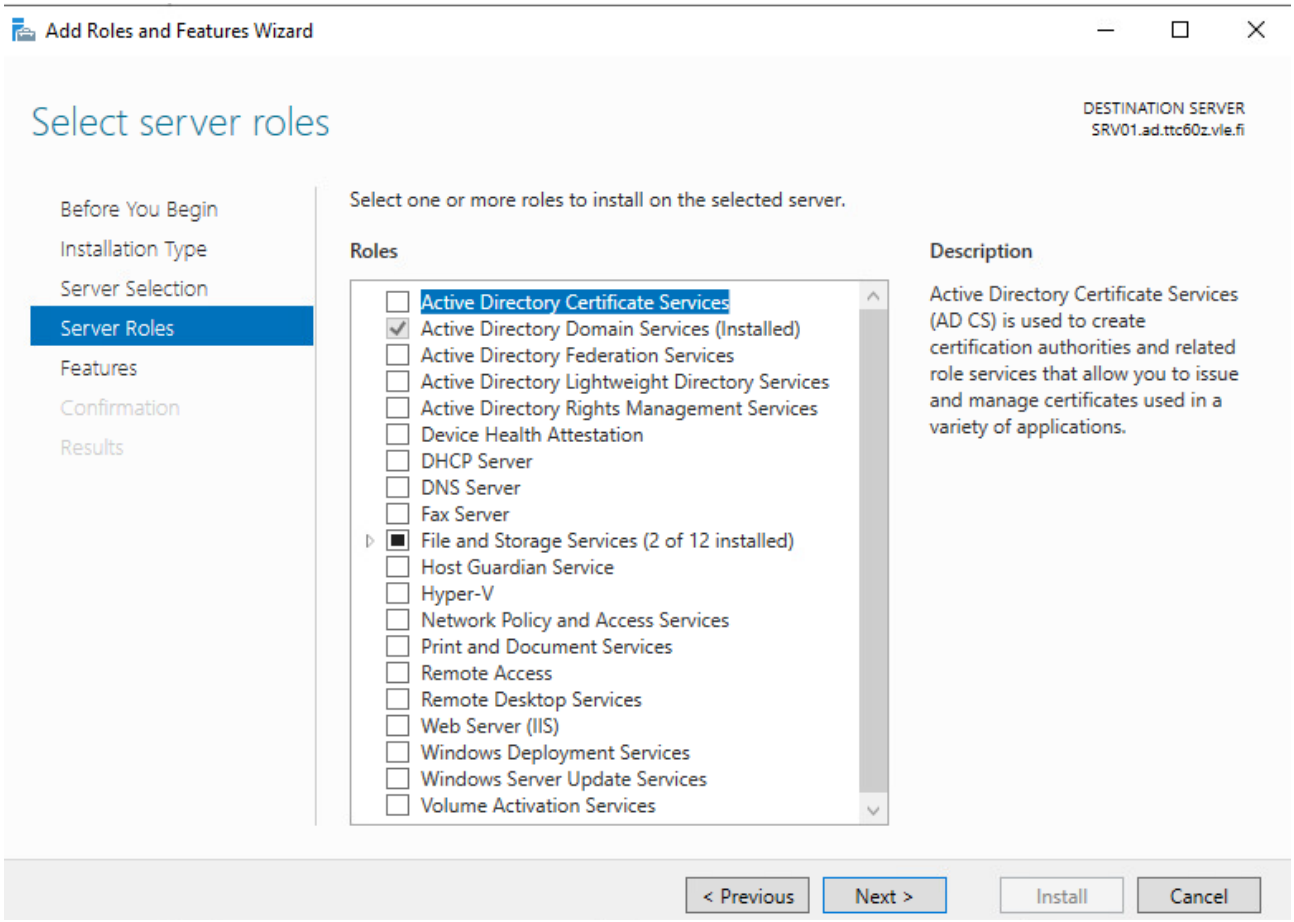


Figure 7. Server Roles

In the Features section, we did not select anything and proceeded directly to the Confirmation section, where we chose "Restart the destination server automatically if required," as before. Now all necessary features and roles were installed. Thus, we removed all unnecessary components, leaving only those features and roles required for file server use.

Following the instructions, we then created a shared folder as shown in Figure 8. (Figure 8.)

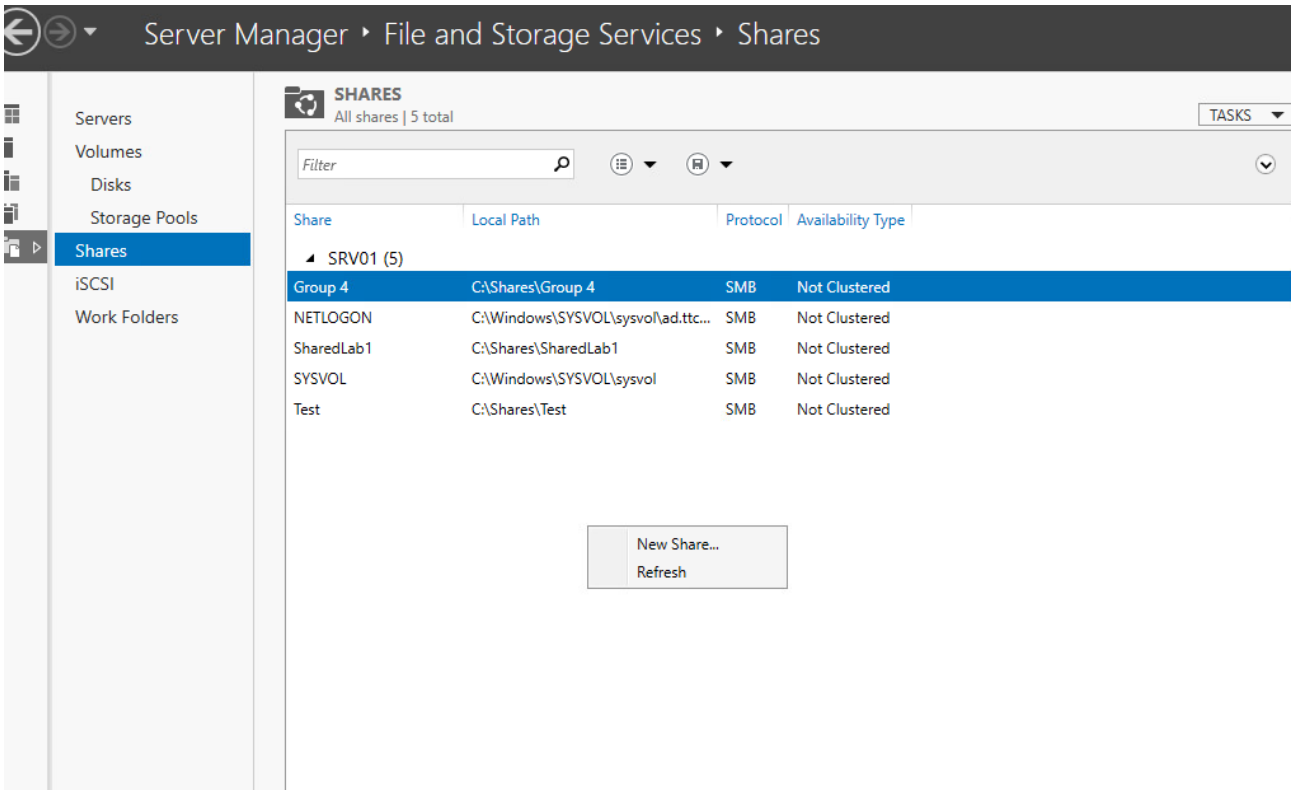


Figure 8. New Share

We selected the "SMB Share – Quick" profile. We did not change anything on the Share Location tab, though it was possible to choose a different storage location on the server instead of the C drive. (Figure 9.)

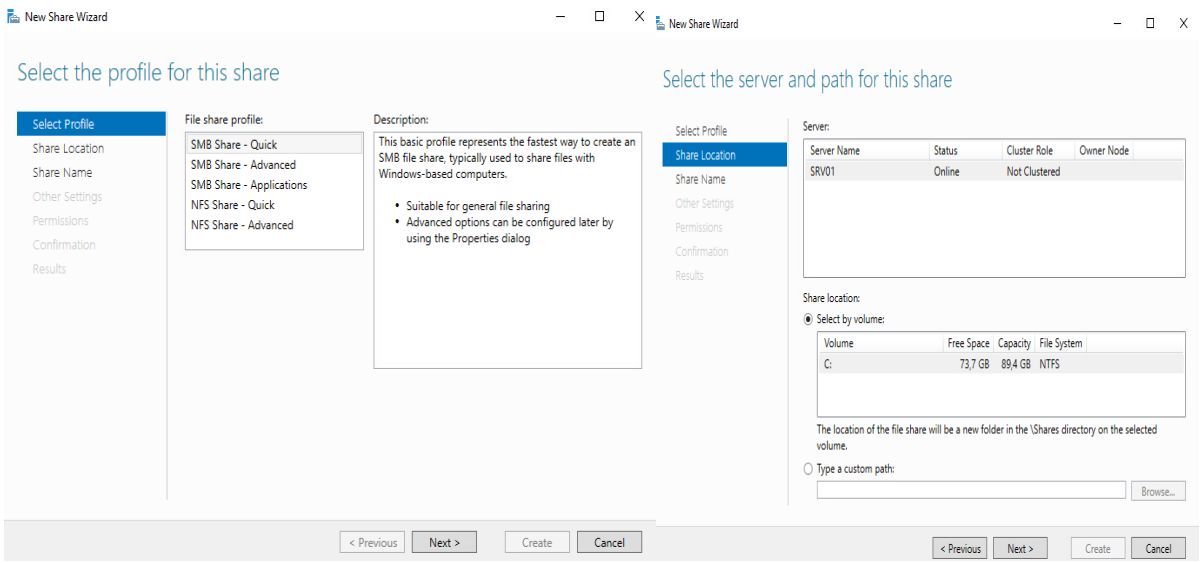


Figure 9. Share Wizard

On the Share Name tab, we assigned the folder a name and provided a description. Since we were creating our first folder and practicing its setup, we named the folder "Test." Here, we set the path that remote users would use to access the folder, specifying it as \SRV01\Test. (Figure 10). We proceeded to the **Other Settings** tab, where we selected security-critical options such as **Enable access-based enumeration** and **Encrypt data access**. We chose these settings because they help protect data by ensuring that unauthorized users cannot see or access information that does not belong to them. (Figure 10.)

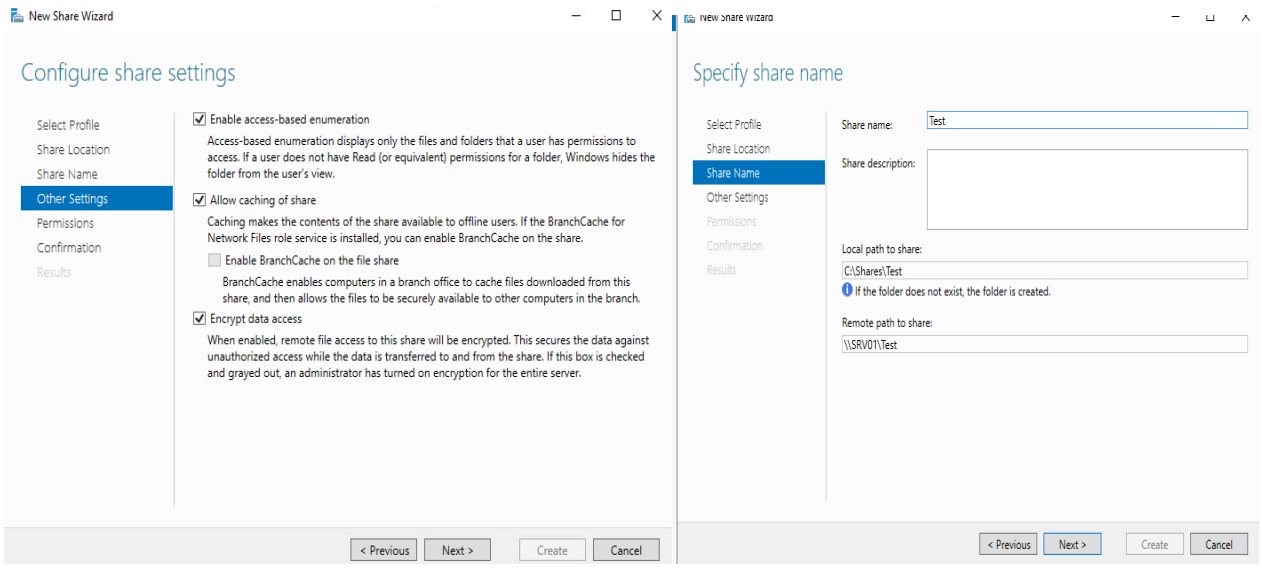


Figure 10. Share Name and Other Settings

On the **Permissions** tab, we defined the users and user groups that have access to the shared folder. These permissions can be adjusted after creation as well, which is what we did. This allows for flexibility in managing access as the needs of users and security requirements evolve.

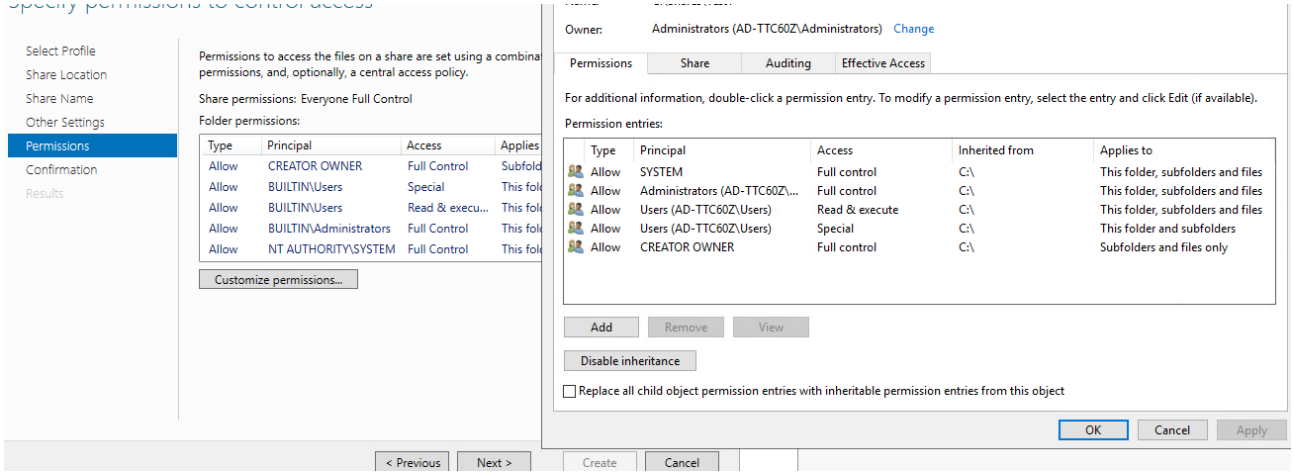


Figure 11. Permissions

On the **Confirmation** tab, we double-checked that all settings were correct and then clicked the **Create** button to create the folder. This step ensures that all configurations are finalized and implemented as specified before the folder goes into use.

We added a test user to the list of users who have the right to see the folder. As shown in Figure 12, the folder was located at the previously specified path \SRV01, when we logged onto the WS01 machine as the test user. This demonstrates how the permissions and network path settings function in a real-world scenario, ensuring that only authorized users can access the designated resources.

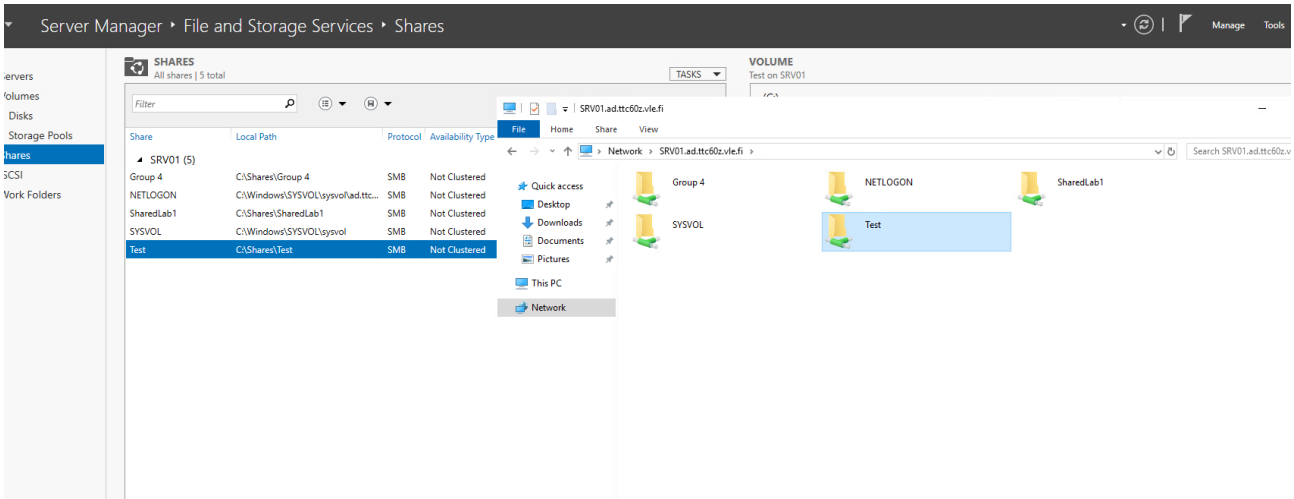


Figure 12. Test user on network drive

2.2 Active Directory Hardening

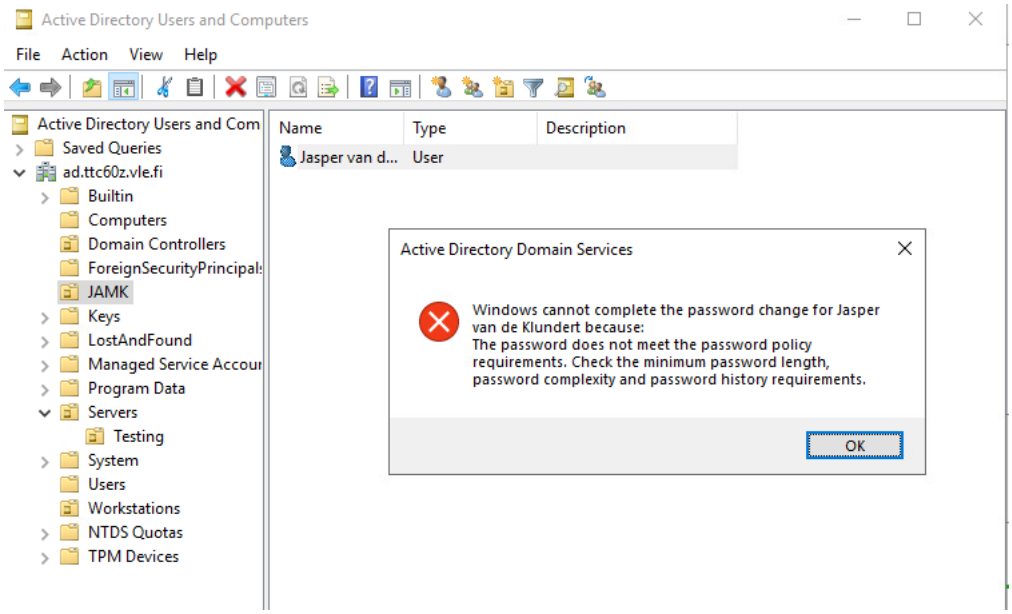


Figure 13. AD Hardening

2.3 GPO Hardening

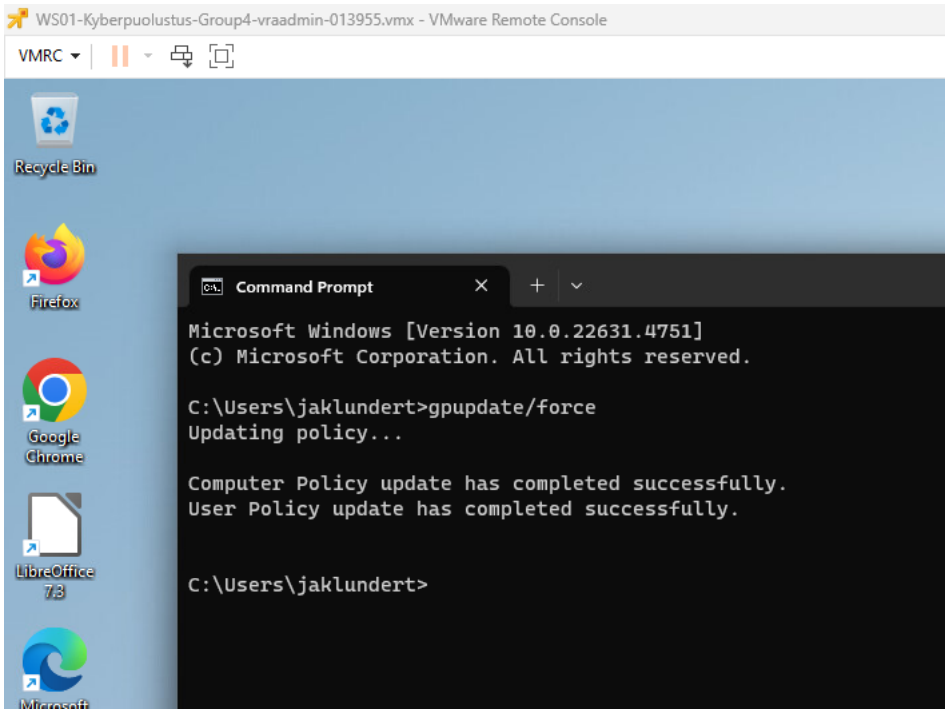


Figure 14. GPO Hardening

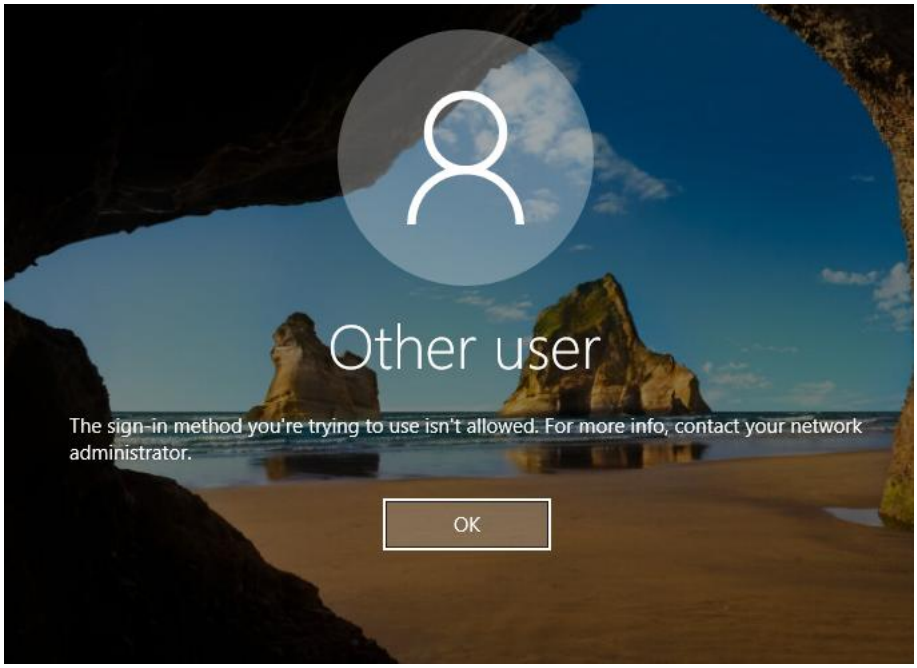


Figure 15. Testing Other User Authorization

3 Conclusion

The first lab work on hardening was a good initial introduction to the process. There were numerous hardening guides available, and some of them were very extensive, so at first, it felt really difficult to find a guide to follow. Once we accepted that it wasn't practical to do everything from one guide, but instead chose a few key areas, things started to roll. At first, implementing the hardenings felt a bit confusing, but once we dared to click around and experiment, the creation of various rules and restrictions began to make sense.

In the end, the lab left us with a good feeling. After the initial difficulties, we managed to implement some hardenings that we considered important. For example, password practices and application usage restrictions were relatively easy to implement and are useful. We could certainly have done more hardening, and we will probably do more in the future, but within the course schedules, not everything could be completed.

References

Wright, G. ,2023. Definition file server. What is a file server and how does it work?

Chai, W. 2021. Definition Active Directory.What is Active Directory (AD)?

Simister, A. 2024. What is Active Directory? Structure, How It Works & Benefits. What is Active Directory? Structure, How It Works & Benefits

Allen, R. 2023. Account Lockout Policy: Configuration Guide. Account Lockout Policy: Configuration Guide

GeeksforGeeks. Lightweight Directory Access Protocol (LDAP). Lightweight Directory Access Protocol (LDAP) - GeeksforGeeks

Microsoft network server: Digitally sign communications (always), 2023. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/win dows-10/security/threat-protection/security-policy-settings/microsoft-network-server-digitally sign-communications-always

Loshin, P. 2021. Definition Kerberos. What is Kerberos and How Does it Work? - Definition from SearchSecurity

Rendell, D. 2024. Find and fix server problems with Best Practices Analyzer. Find and fix server problems with Best Practices Analyzer | TechTarget

Appendix 2. Title of the Appendix