Lab 6: File and Share Management

Server System Management - Windows Server Labs

SERAFIM CIOBANU

Academic Year: 2022-2023

Table of Contents

[Introduction 3](#_Toc129692465)

[Learning Goals 3](#_Toc129692466)

[Knowledge (what you need to know) 3](#_Toc129692467)

[Abilities (what you need to be able to do) 3](#_Toc129692468)

[Requirements 3](#_Toc129692469)

[File & Share Management 4](#_Toc129692470)

[Extensions - Optional Assignments 8](#_Toc129692471)

## Introduction

This lab will focus on managing files and (shared) folders using the GUI and PowerShell.

## Learning Goals

# Knowledge (what you need to know)

* How are permissions on files and folders configured in a Windows/Active Directory environment
* What protocol, roles and tools do you need to create, manage and access shared resources

# Abilities (what you need to be able to do)

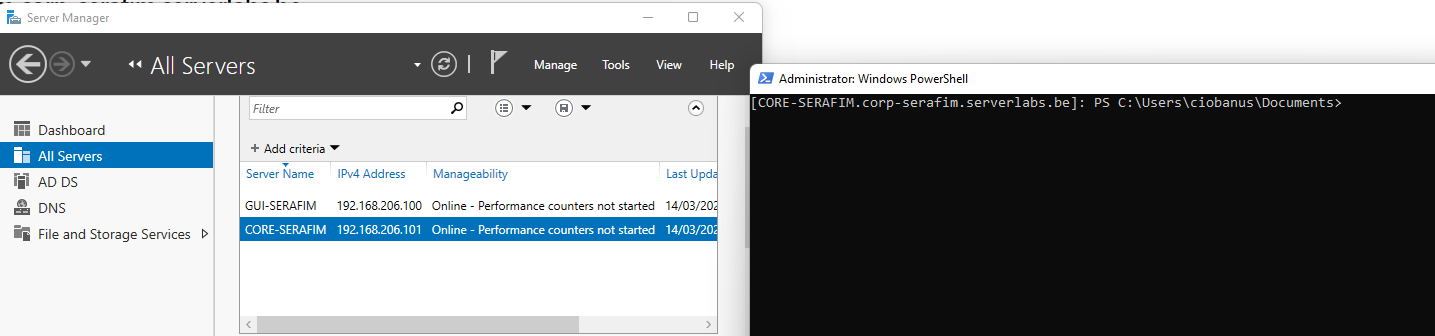
* Create shared objects
* Restrict & give access to shared objects
* Verify effective access on resources (permissions)

## Requirements

Your three Windows VMs (CORE, GUI and WIN11), integrated in the corp-<firstname> domain. You’ll also need the domain users Mickey and Donald that were created in lab 4. All three VMs should be running during this lab. Even though you won’t explicitly log in to the GUI server for most of the lab, it is strongly advised to have it running because it is the AD Domain Controller.

## File & Share Management

1. Sign in to your Windows 11 VM using your personal domain user account and open a remote PowerShell console that connects to your core server. You can for example do this by selecting the core server in the Server Manager tool and then selecting “Windows PowerShell” in the right-click menu. Take a look at the prompt. Is this the same prompt as on your Windows 11 (the custom one)? Is this fixable? We suggest to not use this for screenshots in which you prove you are running everything in your environment.



New-Item -Path $profile -Type File -Force

notepad $PROFILE

function prompt {"`n$(get-date) | PS [$Env:userdomain\\$Env:username@$Env:computername] `n$($PWD.ProviderPath) > "}

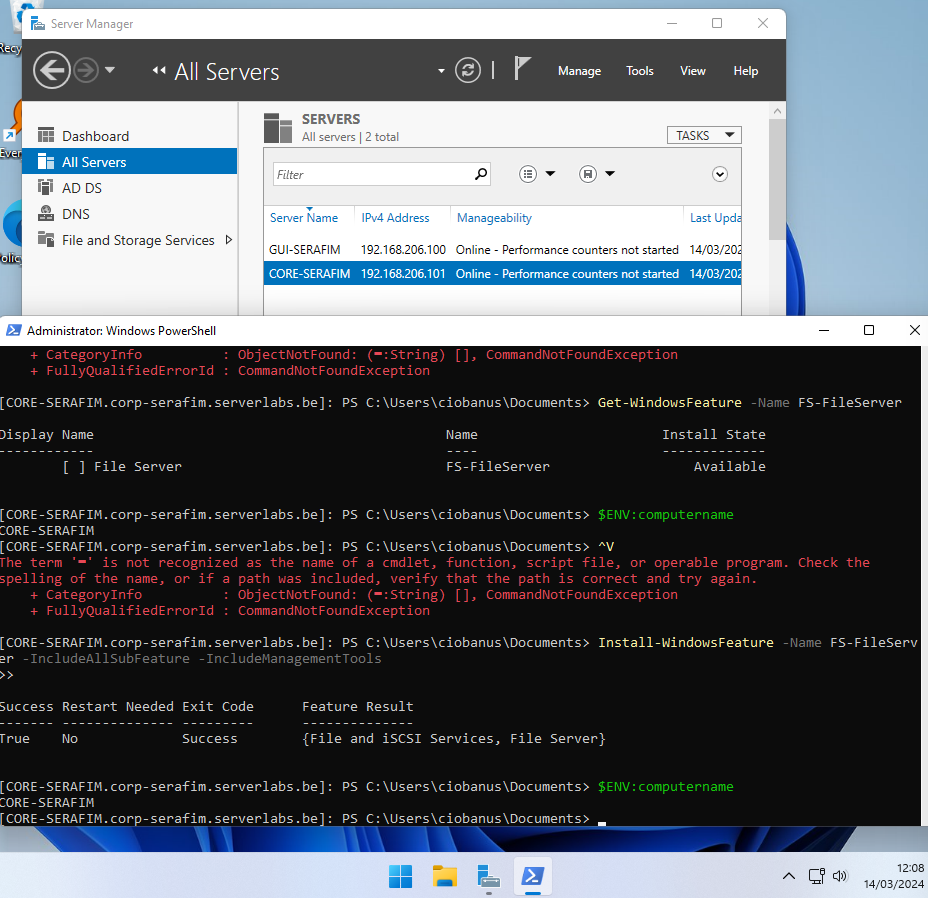
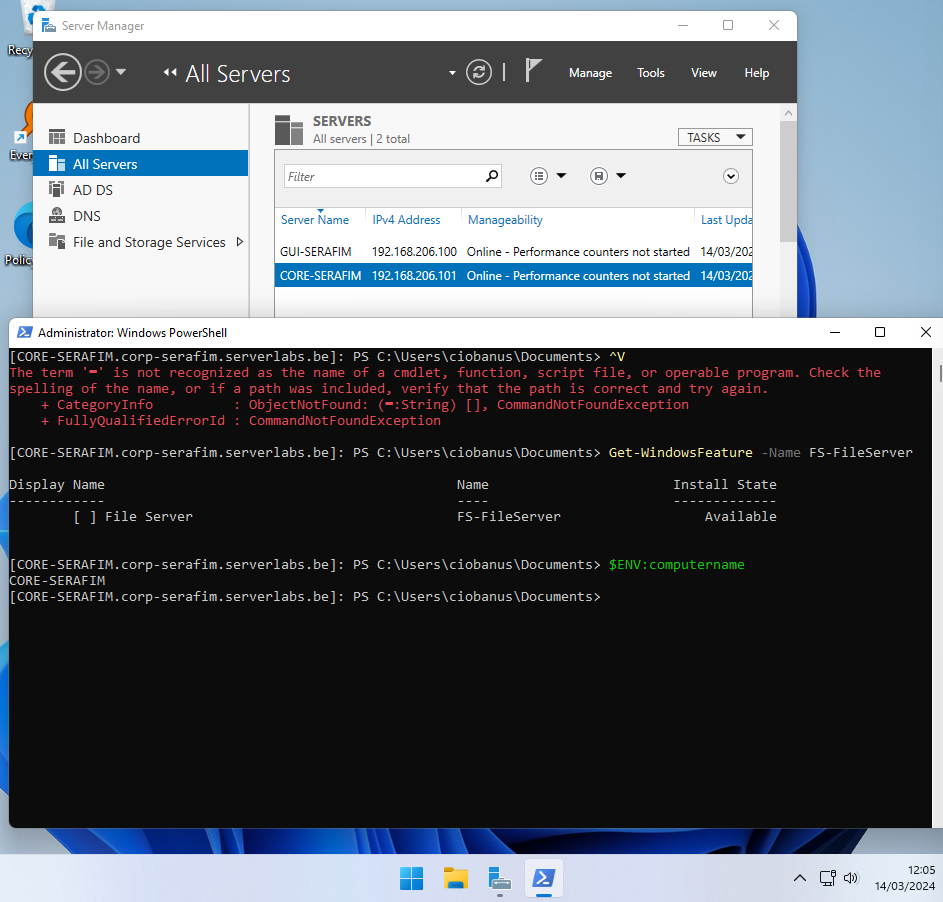
But this does not work!

But it still shows that I am connected to the right PC and with the right user

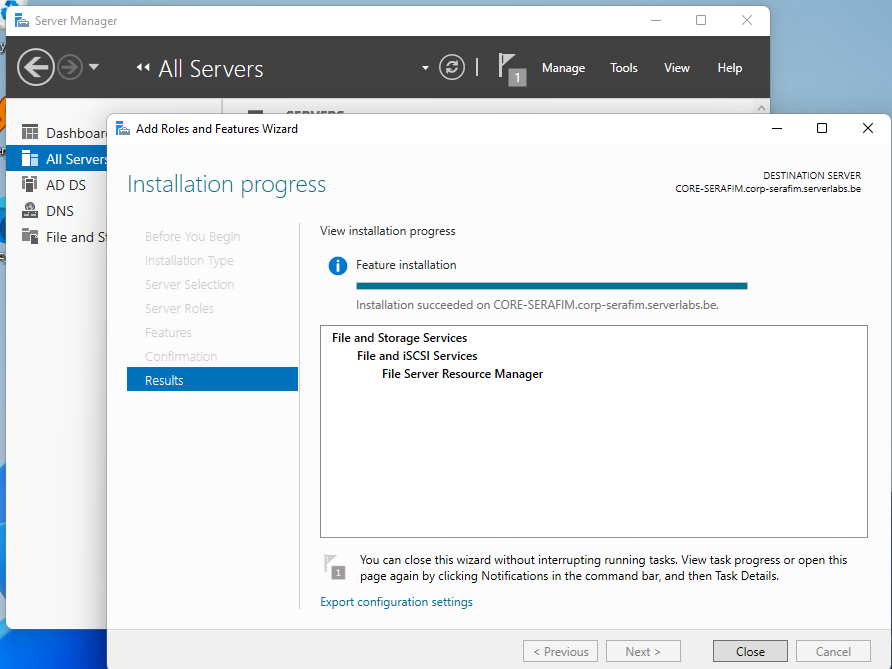
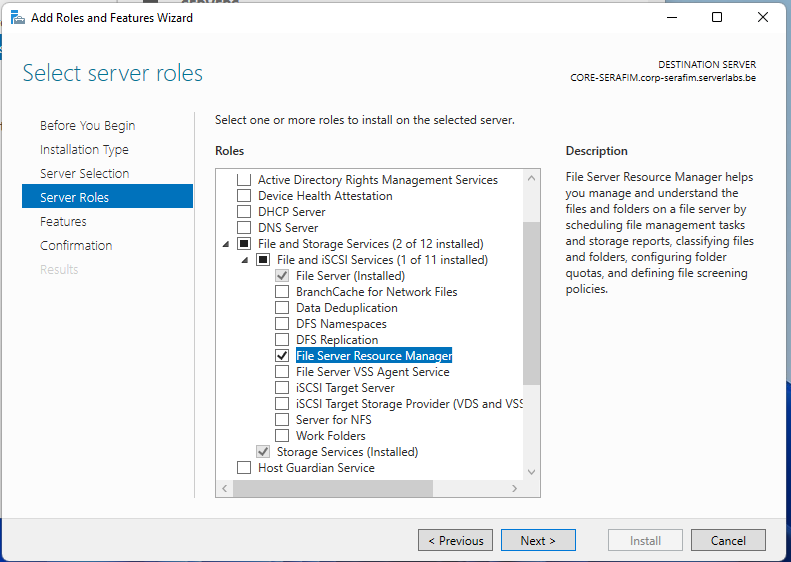
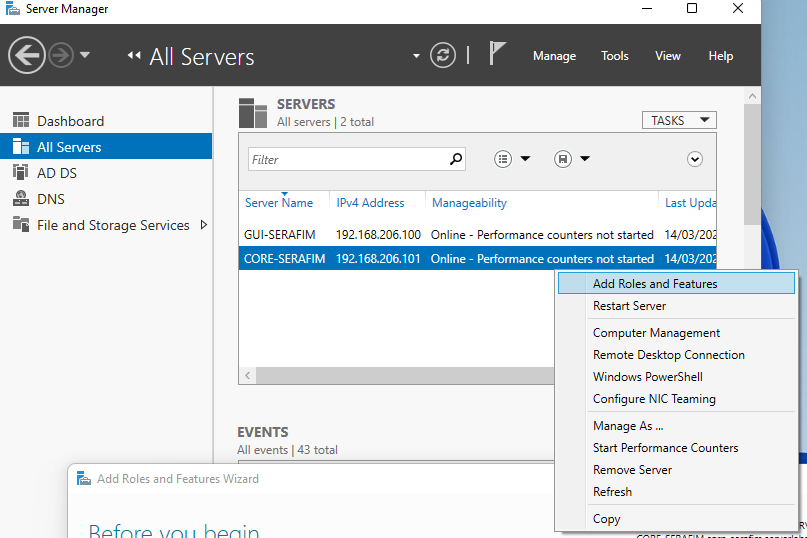
1. Since we will use the core server as a file server in this lab, it is interesting to see if the appropriate roles are installed on your core server. Therefore, check with a PS-cmdlet whether the “FS-FileServer” role is installed on your core server. If it is not installed yet, go ahead and install it with another PS-cmdlet but **beware:** you should also *include the “all subfeatures*” and “*management tools*” options.

Get-WindowsFeature -Name FS-FileServer

Install-WindowsFeature -Name FS-FileServer -IncludeAllSubFeature -IncludeManagementTools

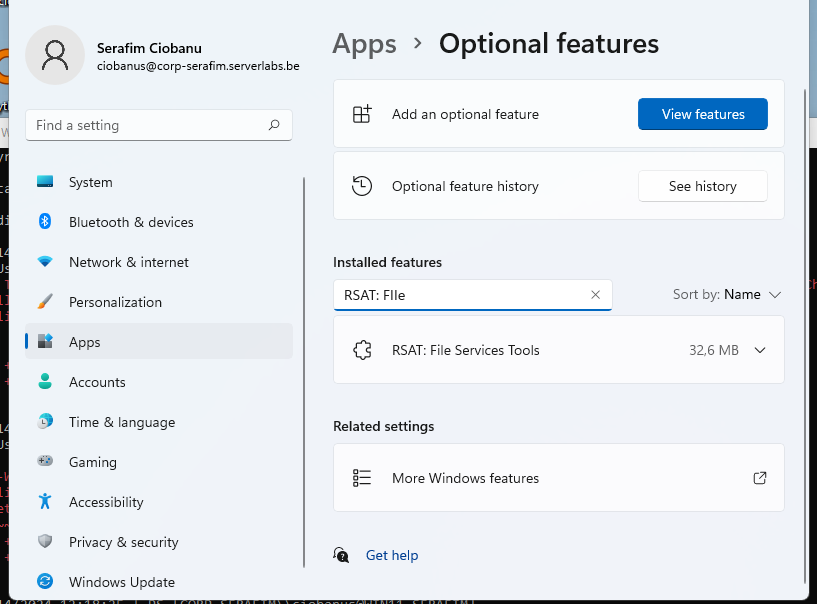


1. Another interesting role is the “File Server Resource Manager”. Use the Server Manager (from your windows 11 VM) to install this role on your core server.

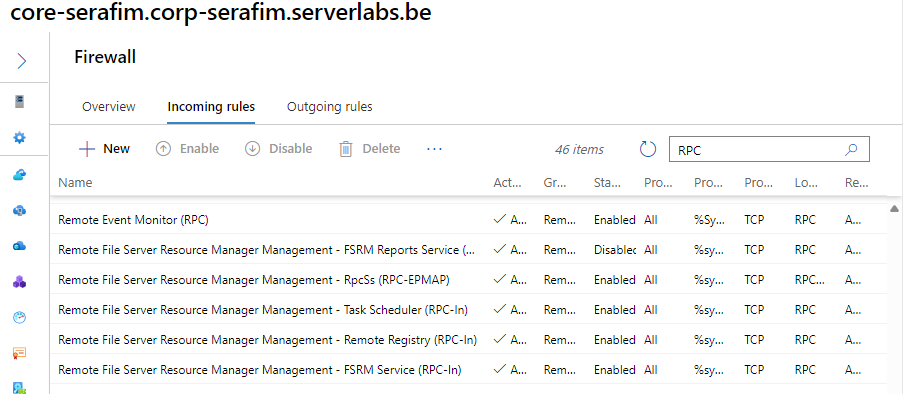
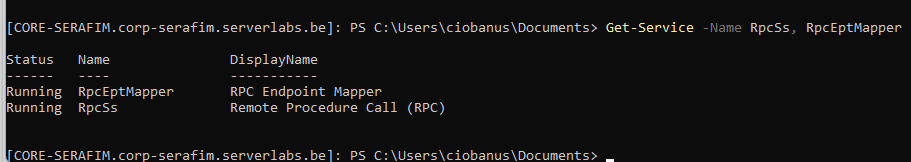
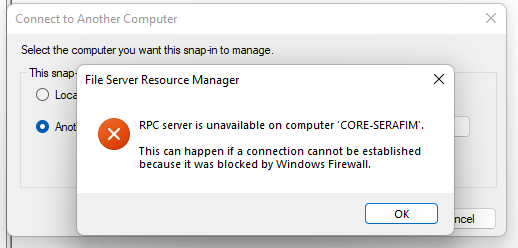
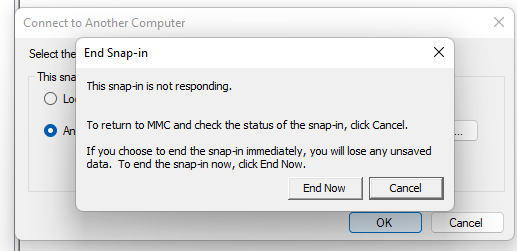
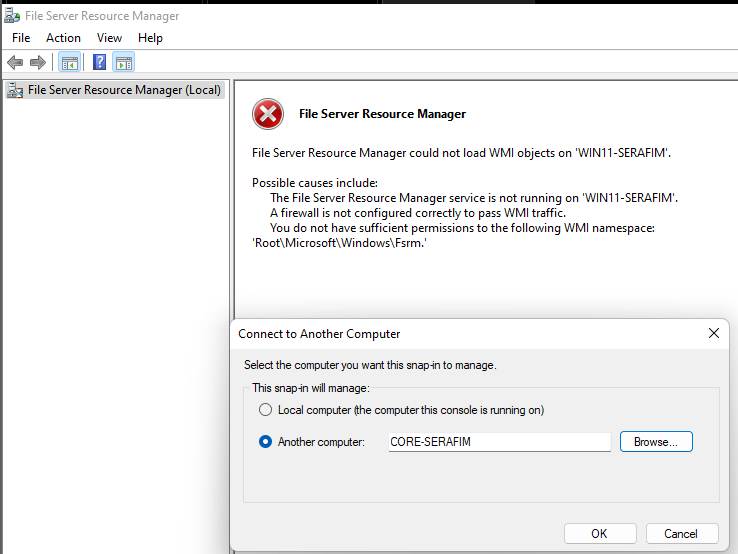


1. To properly manage the file server service from the Windows 11 VM, you will also need to install a corresponding RSAT tool called FileServices on the Win11 VM. You can use PowerShell or the GUI for this.

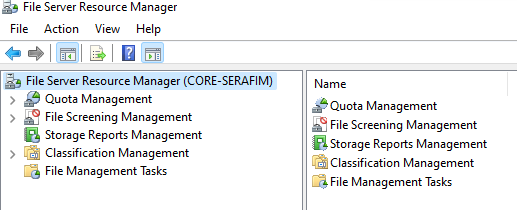
Get-WindowsCapability -Online | Where-Object {$\_.Name -like "\*RSAT\*FileServices\*"}



1. Next, open the File Server Resource Manager console on your Windows 11 VM and connect it to your CORE server. This will not work. Read the error message properly and make the necessary modifications to solve the problem. Put a screenshot below as proof that this works and explore the different Management options. Aside from “Classification Management” and “File Management Tasks” what are the other 3? Afterwards you can close this window.



Ended up enabling more rules that are connected/related to RFSRMM (Remote File Server Resource Manager Management), and now it worked.

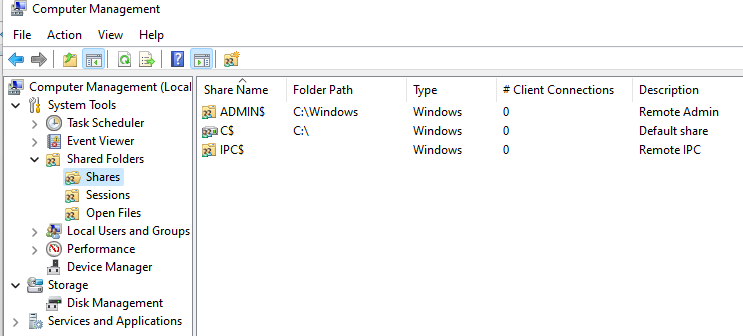


1. Our goal is to provide domain users with a centralised home directory that should be accessible from every computer (so no matter what workstation/client they use, they should be able to access their home directory). To achieve this, you will create a folder “Homedirs” on the CORE server. Create this folder in the root of the C drive of the CORE VM, by using a PS-cmdlet that runs from your Windows 11 VM. Do not create a PowerShell connection for this, but instead run (*invoke)* the command from the Win11 machine.

Invoke-Command -ComputerName CORE-SERAFIM -ScriptBlock {New-Item -Path 'C:\Homedirs' -ItemType Directory}

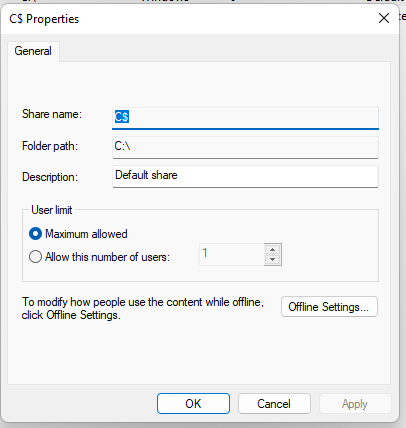
1. View all built-in shared folders on your CORE server via the GUI from your Windows 11 VM. Tip: you can do this with Server Manager or WAC, but the fastest way is to run an .msc-file. Look up the name of that file on the Internet to immediately open the Shared Folders console. How many share names do you see?

compmgmt.msc



I can see 3 share names

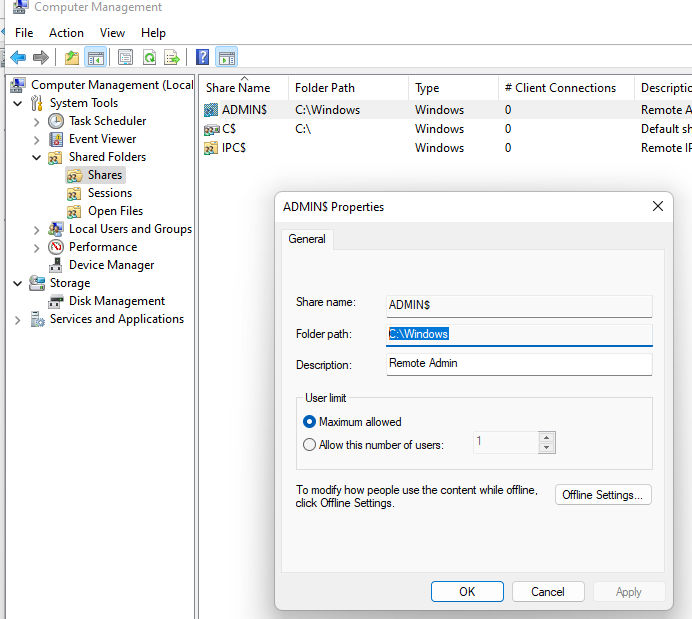
1. Note that the C drive of your Core server is shared. What is the **exact** name of this share and what is the meaning of the special character?



The "C$" shared folder on a Windows system is a hidden administrative share. Hidden shares, also known as Administrative shares, are network shares that are not visible when viewing another computer's shares but are accessible if the name of the hidden share is known. The "$" at the end of the share name indicates that it is a hidden share.

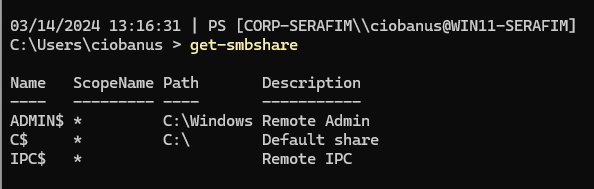
1. Write down the path of the folder that is shared with the name ADMIN$?

C:\Windows



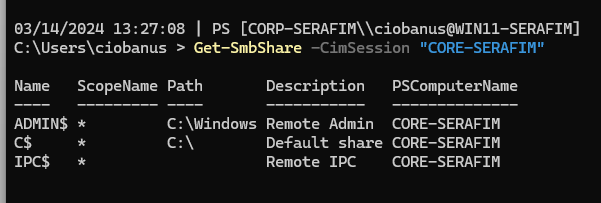
1. Which PS-cmdlets you need to type on your Windows 11 client to see the name and path of all shares defined on
   1. Your local computer (the windows 11 client)?

Get-SmbShare



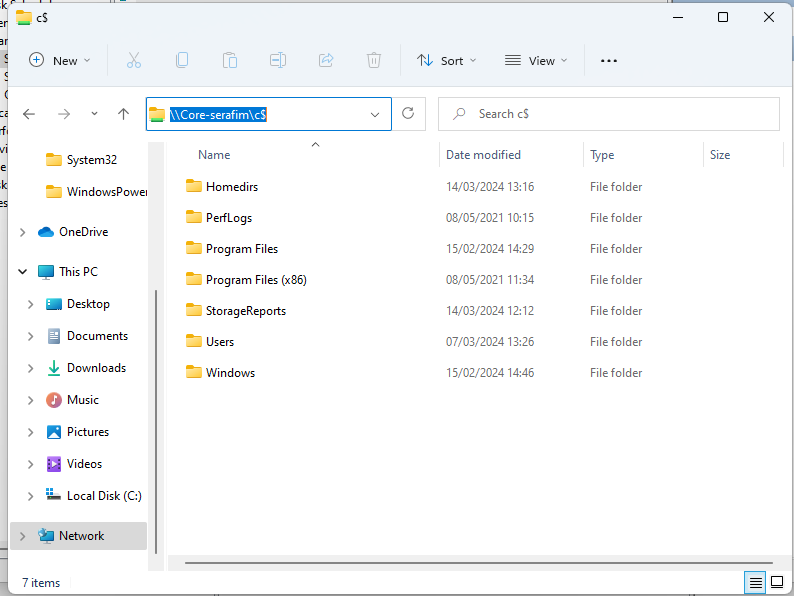
* 1. Your CORE server?

Get-SmbShare -CimSession "CORE-SERAFIM"

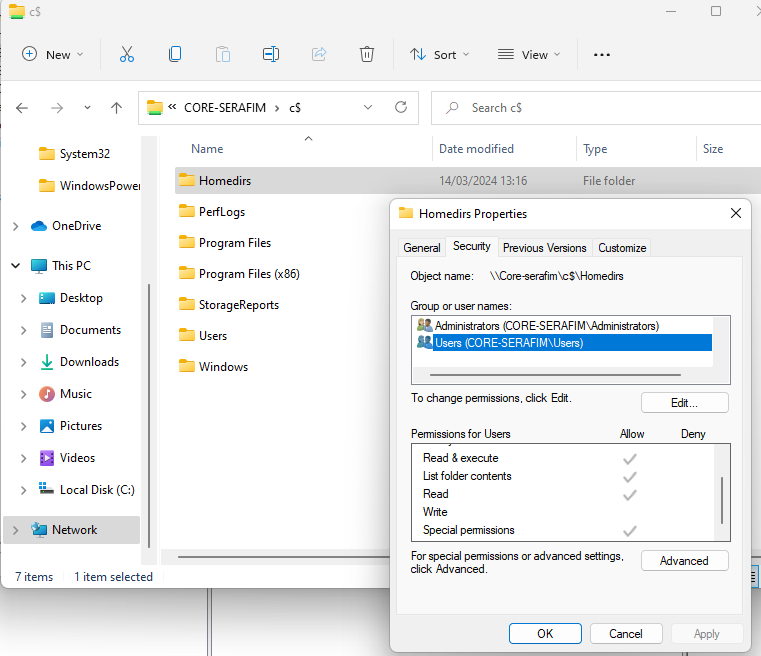


1. To access a shared folder defined on a remote computer, you have to enter the UNC path of that shared folder in the address bar of File Explorer. The general syntax of a UNC path is: \\COMPUTERNAME\sharename or \\IP address\sharename. What do you need to enter in the File Explorer address bar on your Windows 11 VM to access the (hidden) C drive-share of your Core server? Test this!

\\Core-serafim\c$



1. Using File Explorer on your Windows 11, request the NTFS properties of the Homedirs folder on your Core server. What permissions do users in the “Users” group have?



Read & execute

List folder contents

Read

Special permissions

1. Inside the newly created Homedirs folder, we’ll provide each user with their own home directory. To prevent the users from viewing each other’s home directory however, you will first need to modify the NTFS permissions of the Homedirs folder itself as follows. Use the Win11 File Explorer for this.
   1. Remove the permissions on the Users group

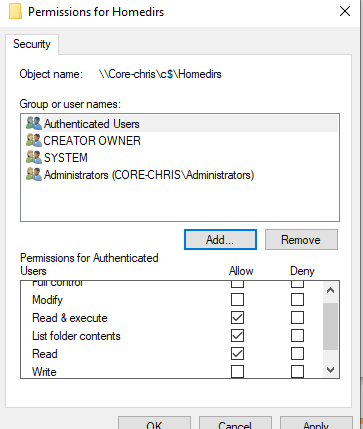
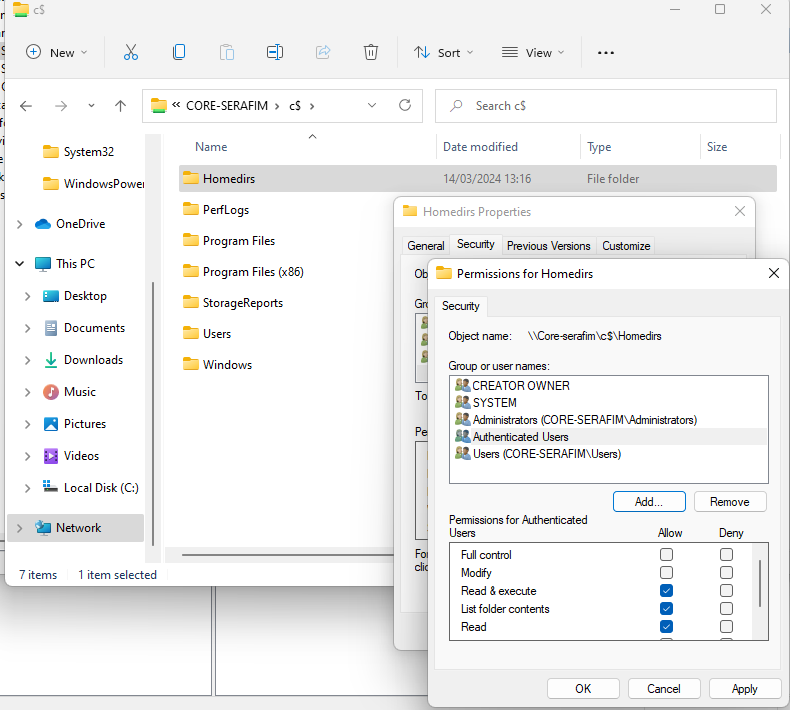
Properties > Security > Disable Inheritancee

Then apply, Edit > Users > Uncheck all allow that can

* 1. Add the authenticated users group to the ACL with the default permission (see screenshot below). **Please note: make sure this permission only applies to the folder itself (and not to files and subfolders)!** (cfr lessons HDOS).

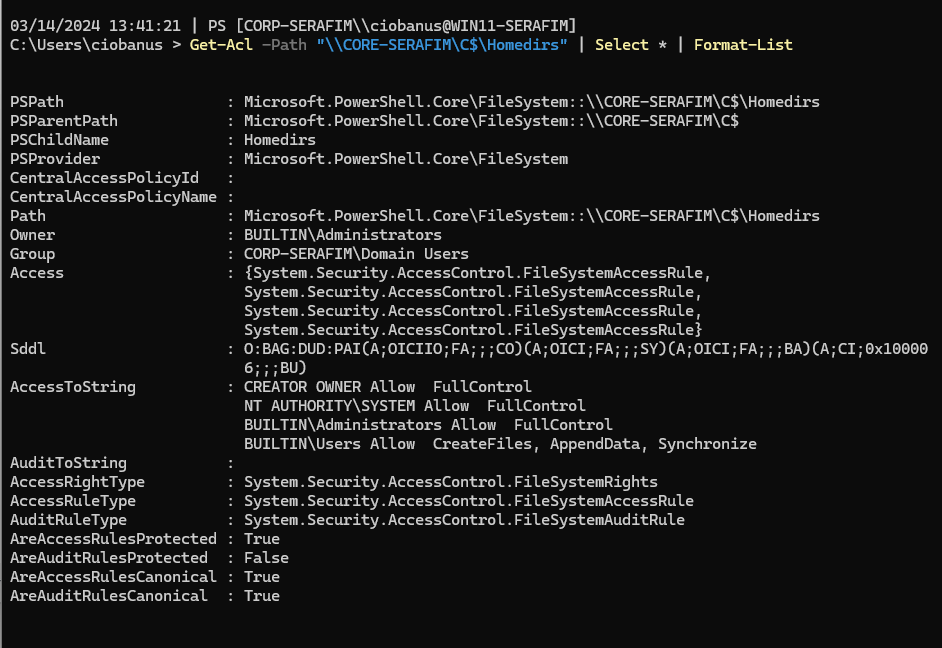
Add > Authenticated Users > Check Names > OK

* 1. Leave all other permissions untouched



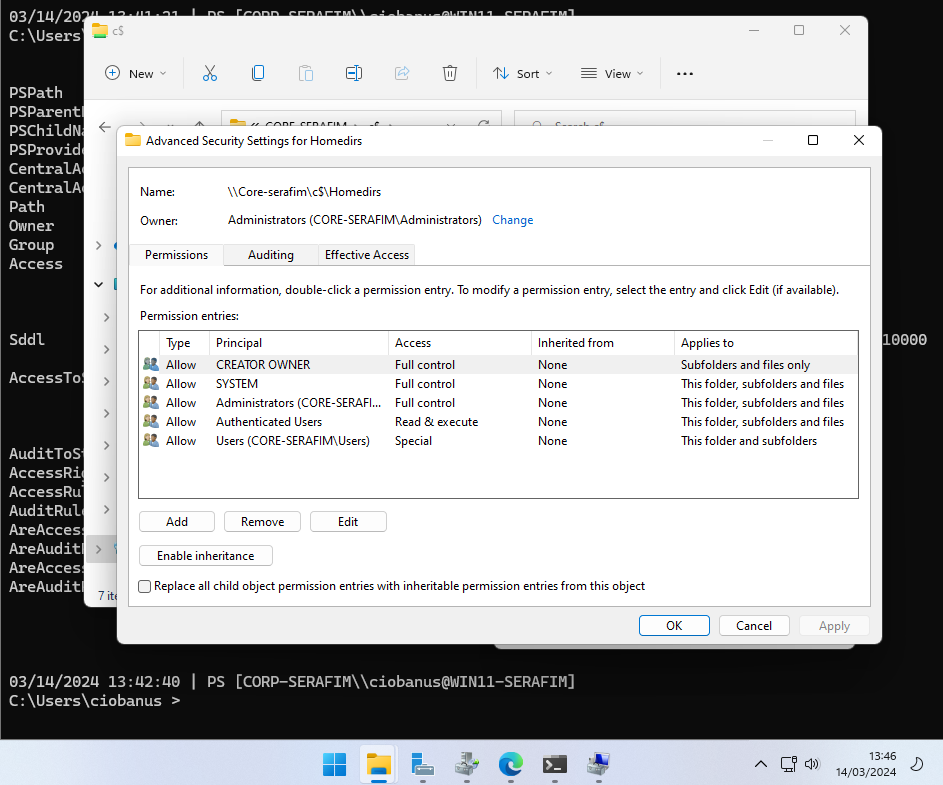
1. On your Windows 11 VM, make use of a PS-cmdlet to request the NTFS permissions on the Homedirs folder in a readable format (use a list format). Paste below a screenshot of the output of your command (and pipe to select \*).

Get-Acl -Path "\\CORE-SERAFIM\C$\Homedirs" | Select \* | Format-List

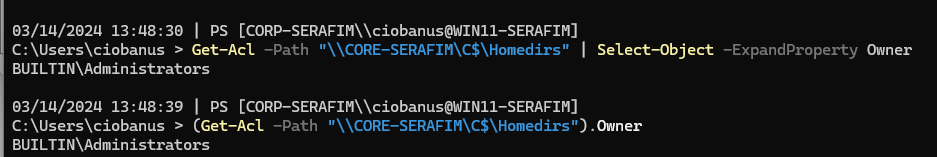


1. On your Windows 11 VM, use File Explorer to request the owner of the Homedirs folder.

Properties > Security > Advanced



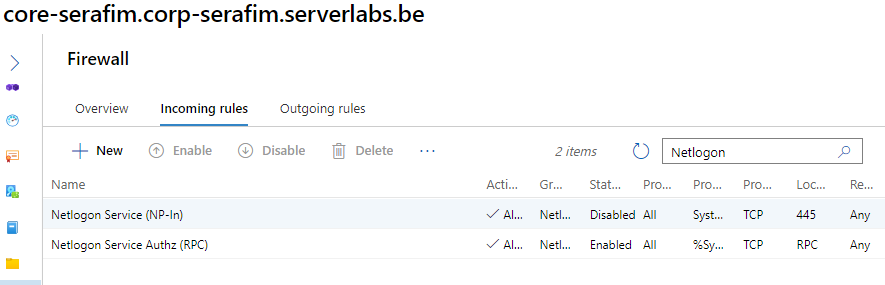
1. On your Windows 11 VM, use a PS-cmdlet to request the owner of that folder.



Get-Acl -Path "\\CORE-SERAFIM\C$\Homedirs" | Select-Object -ExpandProperty Owner

(Get-Acl -Path "\\CORE-SERAFIM\C$\Homedirs").Owner

1. On your Windows 11 VM, make use of File Explorer to view the effective access of Mickey to the Homedirs folder. If this doesn’t work right away. Read the error message carefully and fix the problem. If you work with a Win10 client, you may need your GUI server to change some rules (Win11 users can do this from the Win11 VM). Paste a screenshot down below of the effective access permissions of Mickey on the homedirs folder of the share.



Properties > Security > Advanced > Effective Access > Select User > mickey > Check Names

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Since the Homedirs folder has to be accessible from all network computers, you have to make it a shared folder. To do this, use the Shared Folders management console on your Windows 11 VM and provide the following settings:

fsmgmt.msc

Shared Folder (Right-click) > Connect to Another Computer

Then you can do Shares (Right-click) > New Share

* 1. Name: homedirs
  2. Folder you want to share: the homedirs folder on your CORE server
  3. Description: “contains home directories of all domain users”

A screenshot of a computer

Description automatically generated

* 1. Share permissions: Everyone: full access

Custom > (Tick) Full Control

A screenshot of a computer

Description automatically generated

Note that is not necessarily a problem that we now give “full access” to everyone on the share level. We will later use the NTFS permissions of the different (sub)folders in such a way that access is more strictly controlled for the specific users.

1. Publish the recently shared folder in the Active Directory. Use the Shared Folder management console to do this.   
   To view the shared folder, you need to enable the “Users, Contacts, Groups and Computers as containers” view in the ADU&C console. Create a screenshot of the ADU&C console where the Homedirs-share is clearly visible (click on the CORE-yourname computer to see the published shared folders).

Right-click on the folder > Properties > Publish > Tick Publish this share

A screenshot of a computer

Description automatically generated

1. Use the GUI to find the DN (distinguished name) of the published shared folder. Paste below a screenshot of this DN.

Had to enable Advanced Features View

CN=homedirs,CN=CORE-SERAFIM,CN=Computers,DC=corp-serafim,DC=serverlabs,DC=be

A screenshot of a computer

Description automatically generated

1. Use the PowerShell Get-ADObject cmdlet to find information about the shared folder (provide the DN from the previous question as the input for the identity option). What is the objectclass? Now perform an ldapfilter with objectclass=volume to retrieve the same information. Information about LDAP filters can be found online.

Get-ADObject -LDAPFilter "(objectClass=volume)"

The class is **volume**

A screen shot of a computer code

Description automatically generated

1. Use the GUI to change the properties of domain user Mickey so that he can use the drive letter H to connect to his personal home folder. Tip: use the appropriate UNC path for a subfolder “mickey” in Homedirs.

A screenshot of a computer

Description automatically generated

Had to change it, because I specified the full path, and not like a “resolver” of that path

\\CORE-SERAFIM\homedirs\mickey

A screenshot of a computer

Description automatically generated

1. Make use of a PS-cmdlet to perform the same thing for Donald as the previous question but choose Driveletter I (i) and subfolder “donald” in Homedirs.

My Donald Duck user was somehow not there, so I created him again with command from Lab 4

New-ADUser -Name "Donald Duck" -GivenName "Donald" -Surname "Duck" -Office "Disney Castle" -AccountPassword (ConvertTo-SecureString -AsPlainText "Friday13th!" -Force) -Enabled $true -Path "OU=Disney,DC=corp-serafim,DC=serverlabs,DC=be" -UserPrincipalName "donald" -SamAccountName "donald"

Set-ADUser -Identity "Donald" -HomeDrive "I:" -HomeDirectory "\\CORE-SERAFIM\homedirs\donald"

A screenshot of a computer screen

Description automatically generated

1. Sign out on your Windows 11 VM and log in again, but this time as Mickey. Open file explorer, and check if the H-drive exists and points to the home folder. Test Mickey’s access (write) rights by creating a file “firstname.txt” (replace firstname by your own name) in the H-drive. This should work.

A screenshot of a computer

Description automatically generated

1. Log in as Donald, and create a text file “donald.txt” in his home folder.

A screenshot of a computer

Description automatically generated

1. Log in as Mickey again, and use file explorer to navigate to the common Homedirs share (use its UNC as path). Can Mickey **see** Donald’s homefolder? Can he **open** it?

A screenshot of a computer

Description automatically generated

Yes, he can, if full path specified \\CORE-SERAFIM\homedirs\

1. To prevent users from seeing files and folders to which they have no access, you need to enable the access-based enumeration on the Homedirs share.   
   Log in as your personal domain user on the DC (GUI server) or the Win11 VM and use Server Manager > File and Storage Services to set this up. Afterwards verify the setting by logging off and logging back in as Mickey on the Win11 VM. If everything works as intended, Mickey should now only be able to see his own homefolder.

A screenshot of a computer

Description automatically generated

1. Log off on your WIN11 client and log back in with your personal domain user.
2. We would like all domain users to use a **roaming profile**. Such a profile allows users to share their (favourite) settings across domain workstations/computers. To achieve this, you will have to create a folder on a file server. Once again we choose the core server. Therefore, create a folder named Profiles on your CORE server (in the root of the C: drive). Do this once again by invoking a PS cmdlet.

Invoke-Command -ComputerName CORE-SERAFIM -ScriptBlock {New-Item -Path 'C:\Profiles' -ItemType Directory}

1. Change, using the File Explorer, the NTFS permissions of the Profiles folder:

Navigate to the \\CORE-SERAFIM\C$

* 1. Remove the permissions on the Users group

I disabled inheritance, and then then removed the user groups

* 1. Add the “authenticated users” group to the ACL with the basic Modify permission. **Make sure this permission only applies to the folder itself (and not to files and subfolders)!**

Needs to be specified in advanced settings!

* 1. Leave all other permissions untouched

A screenshot of a computer

Description automatically generated

1. Create in the Profiles folder a subfolder named “mickey” with the following properties:
   1. Name: Mickey.v6 (the extension .v6 is necessary for roaming profiles used on Windows 10/11 computers)
   2. Permissions: add Mickey to the ACL with the basic “Modify” permission

A screenshot of a computer

Description automatically generated

By default it does not put the **Modify** permission, hence I guess I had to enable it additionally.

* 1. Leave all other permissions untouched
  2. *Note: if, as an administrator, you do not first create the profiles folder of your users, you might not have proper access to those folders afterwards.*

1. Create a shared folder on your CORE server, using a PS-cmdlet (once again if needed by using the invoke-command cmdlet). The shared folder should have the following properties:
   1. Name: profiles
   2. Folder you want to share: The profiles folder, which you created before
   3. Description: “contains the roaming profiles of all domain users”
   4. Folder enumeration mode: access-based
   5. Everyone should have full access rights to this share (like we did for the HomeDirs share earlier)
   6. Verify in the GUI

New-SmbShare -Name "profiles" -Path "C:\Profiles" -Description "Contains the roaming profiles of all domain users" -FolderEnumerationMode AccessBased -FullAccess Everyone

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Publish the recently shared folder in the Active Directory and check if you can indeed find the share in the ADU&C console.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. By default, new users have a local user profile. Let’s change this type for Mickey & Donald to a roaming profile.
   1. Select both users in the ADU&C console.
   2. Select properties
   3. Browse to the tab Profile and fill in the correct UNC-path that will work for both users. Tip: %USERNAME%
   4. Note that the UNC path should not contain the .v6 extension!

A screenshot of a computer

Description automatically generated

1. Sign out of your windows 11 client and log in with the Donald account. Create a folder named “firstname” (replace this by your own name) on the desktop and log out.
2. Sign back in with your personal domain user account. If everything went according to plan, you will find the folder you created in the previous exercise in the Desktop folder of the roaming profile of Donald **on the core server** (share). Check this in the File Explorer! Paste below a screenshot of your Explorer window with the path and contents of Donald’s desktop folder as proof.

A screenshot of a computer

Description automatically generated

I had quite some problems to make it work, as I had issues with the permissions for the folders themselves. The Profiles was setup more or less correctly, but I could not see the Donalds folder (probably because Authenticated Users was not a part of the permissions tab). For Mickey, it was probably inherited, or it was because I created it myself. But the donalds one, did not. I fixed it by manually adding the authenticated users from the donalds account. There sure is some work around that I did not do, but should have done.

1. Because roaming profiles are also stored on all computers that a user has logged in to, you should be able to find the folder you created on the Windows 11 VM. Paste below a screenshot of your Explorer window with the path and contents of that folder as proof. Tip: normally you don't have access to that folder, but you are an administrator ;)

A screenshot of a computer

Description automatically generated

1. Create a shared folder called “Disney90s” on the C drive of your core server. Make sure the share and folder permissions are set in such a way that only users in the Agrabah & Pride Lands group have access. Make sure administrators continue to have full control access. You can do this in 2 steps (dir creation & smb-share creation). Verify the full control access in the GUI.

Invoke-Command -ComputerName CORE-SERAFIM -ScriptBlock { New-Item -ItemType Directory -Path "C:\Disney90s" -Force }

A screenshot of a computer

Description automatically generated

While creating, I said that only Administrators have full rights, and nobody else can do anything

Here I edited advanced security, and disabled simple users, and left it only for Agrabah and pride lands

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Had some issues with the groups themselves (pride lands and Agrabah), all the permissions where set (for the folder), but had to also add them explicitly for the share itself

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Once again finish by performing the **pester** script on leho.

## Extensions - Optional Assignments

* Use Wireshark to monitor traffic when accessing resources over a network. What do you see?
* Write a PowerShell script that asks for
  + A (share)name
  + The name of a group

The script should create a shared folder with the given name & that is only accessible for the given group (and administrators).