Lab 5: Group Policy Management

Server System Management - Windows Server Labs

Serafim Ciobanu

Academic Year: 2023-2024

Table of Contents

[Introduction 3](#_Toc129077450)

[Learning Goals 3](#_Toc129077451)

[Knowledge (what you need to know) 3](#_Toc129077452)

[Abilities (what you need to be able to do) 3](#_Toc129077453)

[Requirements 3](#_Toc129077454)

[Group Policy Management 4](#_Toc129077455)

[Fun with GPOs – Defining some new policies 6](#_Toc129077456)

[GPO Inheritance and Precedence – When do specific GPOs apply? 10](#_Toc129077457)

[Policy simulation – making sure that the right policies apply! 13](#_Toc129077458)

## Introduction

Corporate Windows-based networks typically use Active Directory domains because this allows central management of the user accounts, the servers and client machines, and their respective settings. An important aspect of this is group policy management, which can be used to deploy rules and settings to the domain’s devices and accounts, based on their domain and/or OU membership. In this lab, we’ll take a closer look at Active Directory based group policy management.

## Learning Goals

# Knowledge (what you need to know)

* What is group policy management (GPM), why is it used and how does it work?
* What are Group Policy Objects (GPO), and what are they used for? How are they configured?

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

* Configure group policies

## Requirements

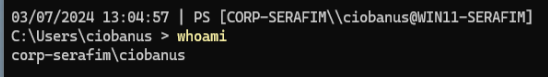
Your three virtual machines in an active directory domain, as configured in the previous labs (lab 1 and 3 are essential, some questions will also require the OUs and user accounts that were created in lab 4)

* Windows Server with GUI (the domain controller)
* Windows Server Core
* Windows 11 client

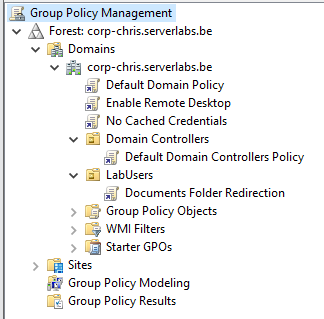
## Group Policy Management

**Important remark:** When performing group policy management (and many other AD configuration operations), scripting can be very useful. Scripting however requires that the (PowerShell) commands are used in a non-interactive way. Therefore, make sure that all the CMD and PS commands that you use in this lab include enough parameters, so they don’t ask for additional information!

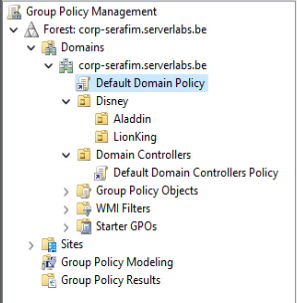
1. Make sure that at least your domain controller (GUI-server) and Windows 11 client VM are running. Preferably, the CORE-server should also be running (even though it is not yet required for the first questions).
2. Sign in to your Win11-VM with your personal domain user account and open the Group Policy Management (GPM) Console. This app can be booted quickly by running **gpmc.msc** (or start it through Server Manager -> Tools -> Group Policy Management)



In the left pane, open the full tree so that all (linked) GPOs are clearly visible and paste a screenshot below (see the figure below for an example). Make sure the name of your domain is clearly visible.



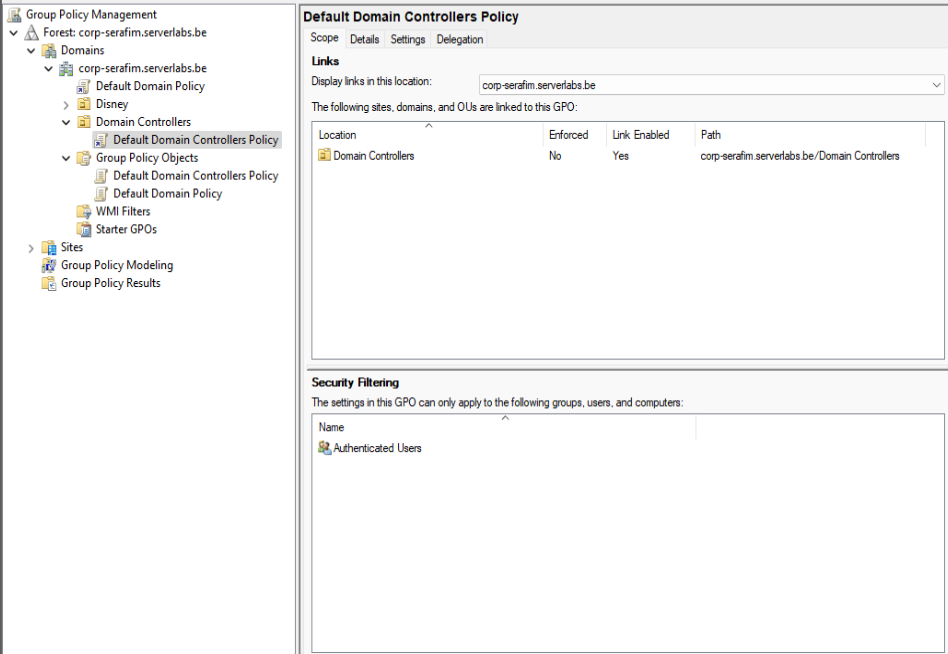
In the “Domains” tree, you’ll see the following:



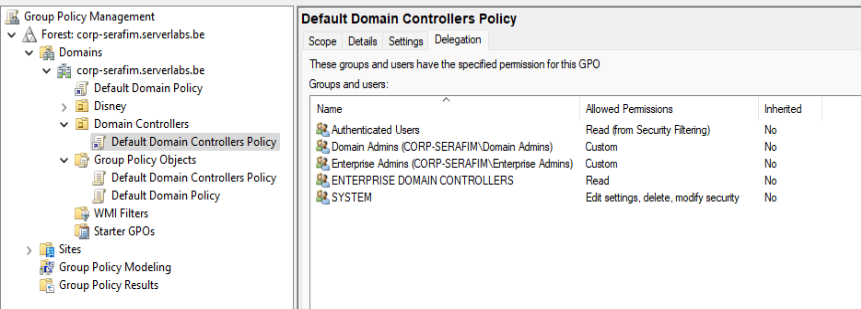
* Your active directory domain and its Organisational Units (OUs), e.g. “Domain Controllers”
* For each container (domain/OU), a list of its linked Group Policy Objects (GPOs) (e.g. “Domain Controllers” à “Default Domain Controllers Policy”
* A separate list of **all** Group Policy Objects, that are defined in the domain
* A list of WMI filters
* A list of starter Group Policy Objects (out of scope for now)

A single GPO can contain multiple group policy settings. Click the “Default Domain Controllers” GPO, and explore the different panes on the right to find out its scope (the linked containers) and the corresponding policies.

* To what container(s) (domain/OU) has this GPO been linked? What is the implication of this (i.e. what computers/users doe it apply to)?

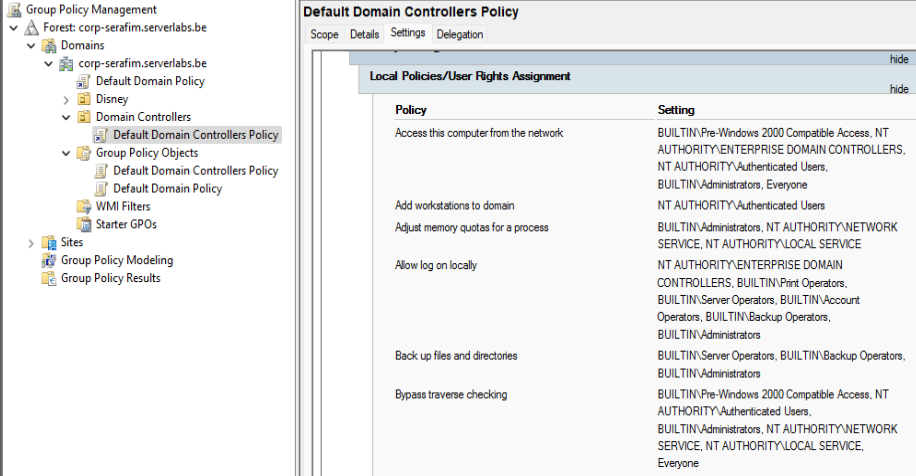


It was linked to the **Domain Controllers** OU, as far as I can understand according to the question. The **Delegation** tab will give more information about the groups it was linked/applied to.

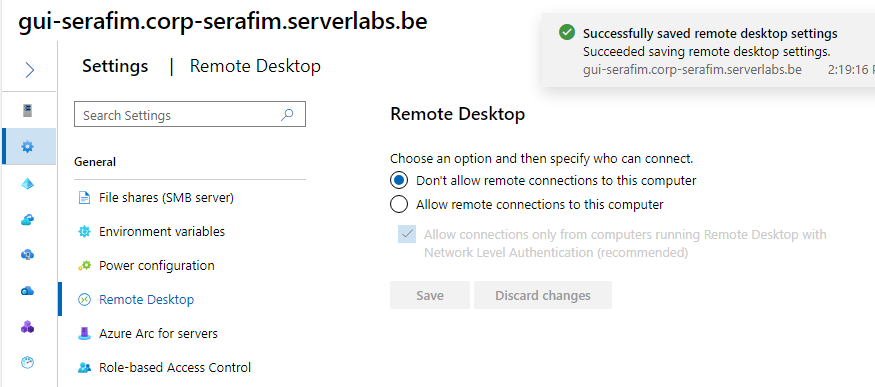
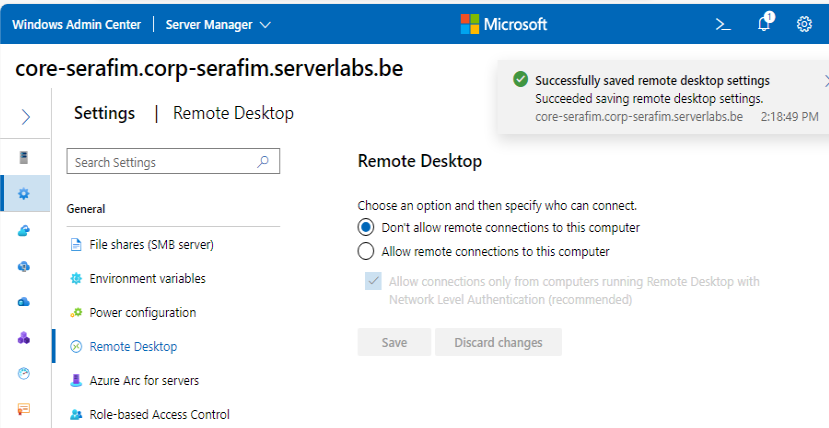
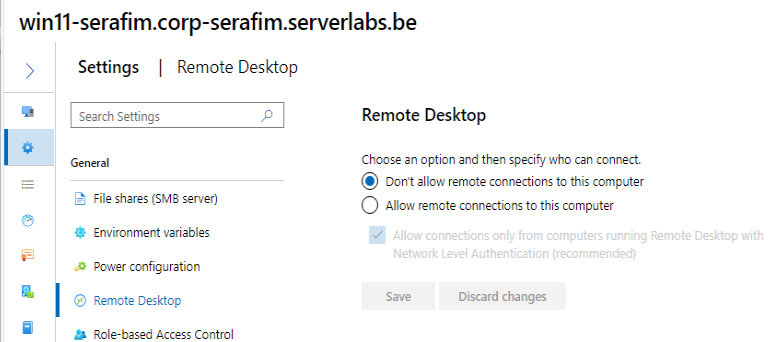


* What users can locally log in to a Domain Controller?

Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies/User Rights Assignment > Allow log on locally



1. Now let’s create our first GPO, that by default turns on the remote desktop server in all the domain computers!
   1. Using Windows Admin Center, disable remote desktop in your three VMs (settings -> Remote Desktop).



* 1. Now we’ll create the GPO. In the GPMC, right-click the “Group Policy Objects” folder for your domain and select “New”. Name the new policy “Enable Remote Desktop”.
  2. Right-click the new GPO and select “Edit”. The group policy management editor will open, in which we will be able to edit the policy configurations for the GPO. These policy configurations are divided into two groups: computer and user configurations. What is the difference between the two?

The main difference lies in what aspect of the system they affect: Computer Configuration applies to the computer itself, while User Configuration applies to the user's environment and settings.

Computer Configuration:

* Policies under Computer Configuration apply to computers or devices themselves, regardless of who logs in to them.
* These policies affect the computer's behavior, settings, and system configurations.
* They are applied during the computer's startup process, before any user logs in.
* Examples of settings that can be configured here include system settings, security options, network settings, and software installation settings.

User Configuration:

* Policies under User Configuration apply to user accounts that log in to the computers.
* These policies affect the user's environment, preferences, and user-specific settings.
* They are applied when a user logs in to the computer.
* Examples of settings that can be configured here include desktop settings, Start menu options, control panel settings, and Internet Explorer settings.
  1. Now find the **four** policies (hint: use the policy overview excel file from Leho), needed to enable remote desktop, and configure them accordingly. These settings should do the following:
     1. Users must be allowed to log in to the computer via Remote Desktop

Computer Configuration → Policies → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Connections.

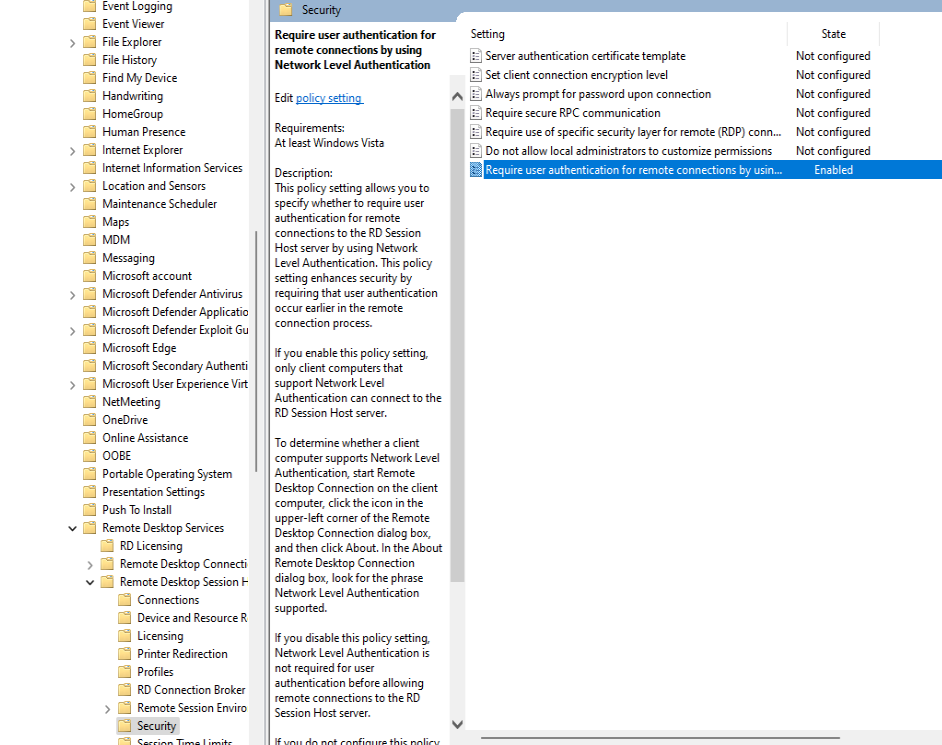
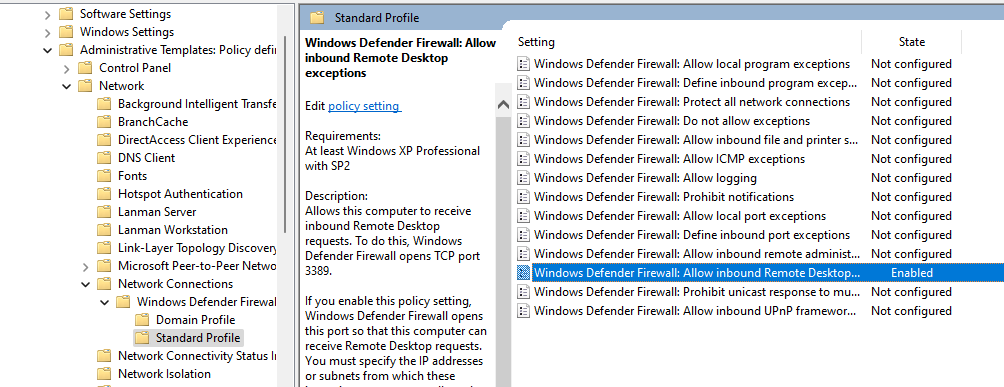
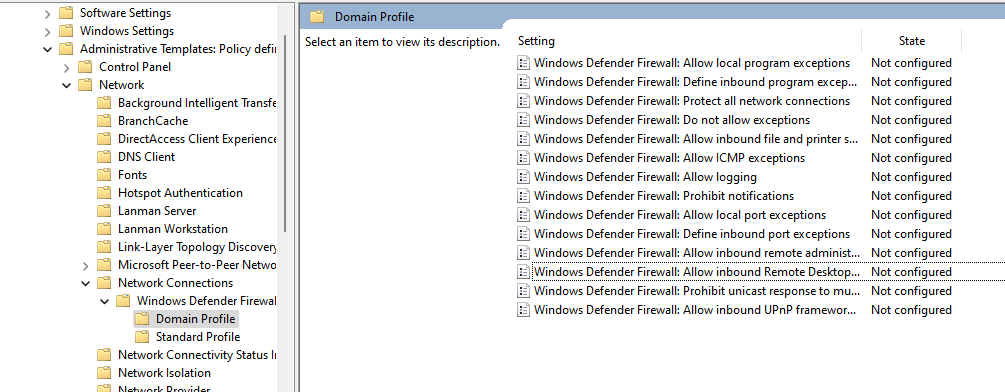
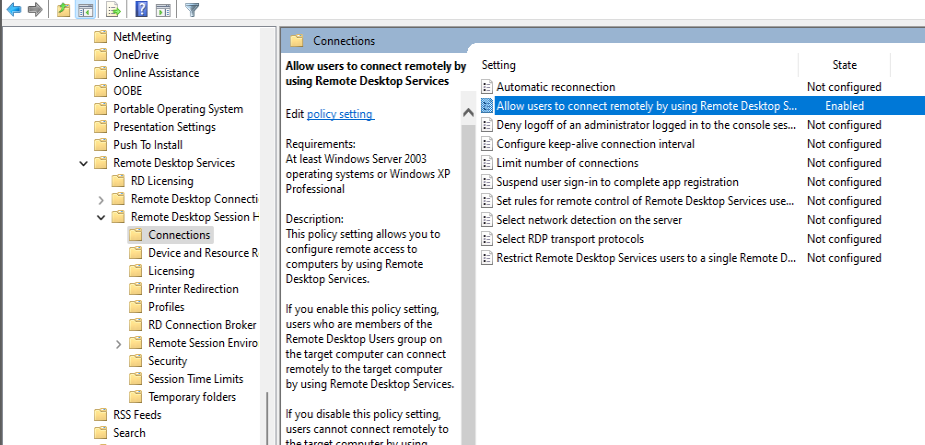
* + 1. As an additional security measure, user authentication is required using NLA (network level authentication)

Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security

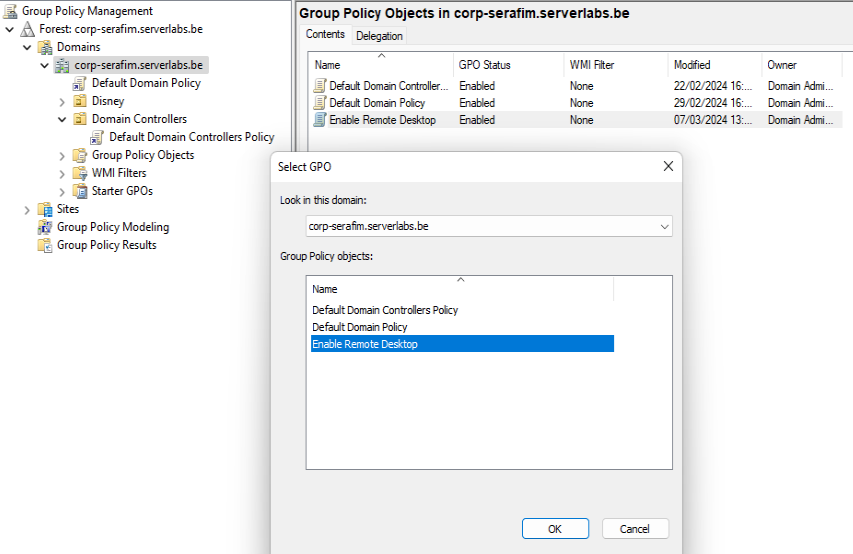
* + 1. Allow “Inbound Remote Desktop” traffic  in the Windows Defender Firewall (both on the domain profile and on the default profile[[1]](#footnote-3))

Computer Configuration > Policies > Administrative Templates > Network > Network Connections > Windows Defender Firewall > Domain Profile.

Paste screenshots for all 4 policies you configured in this GPO.

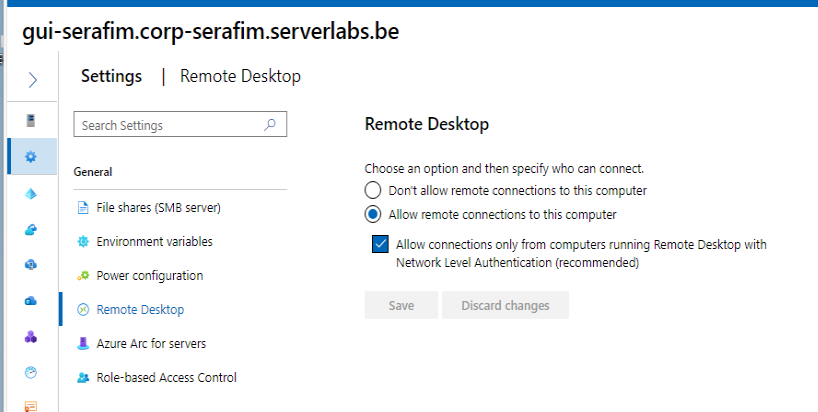
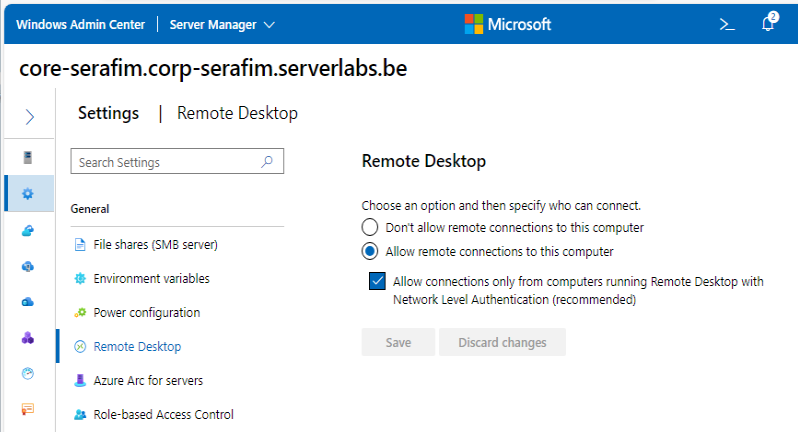
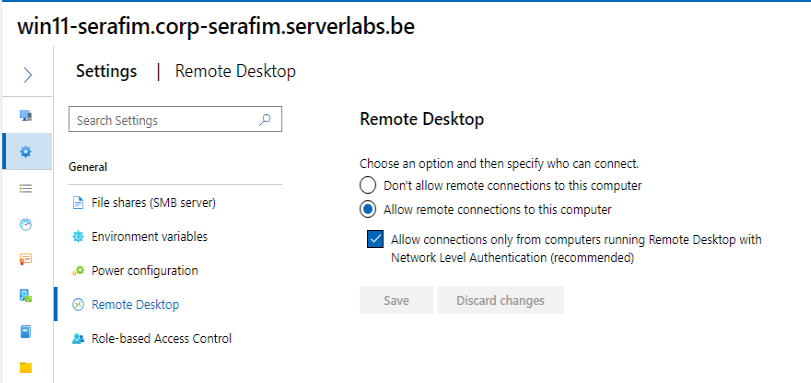


* 1. Next, we need to link the new GPO with its container, the complete domain. Right-click our domain name in GPMC and link to the existing GPO.

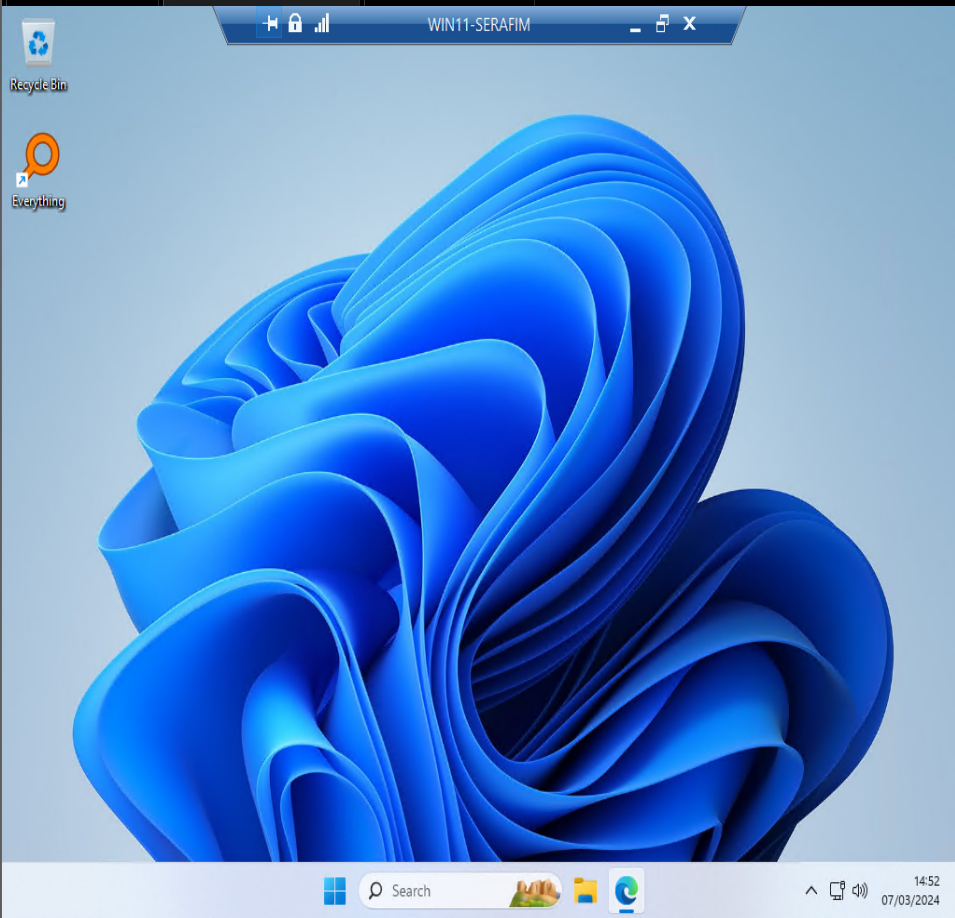
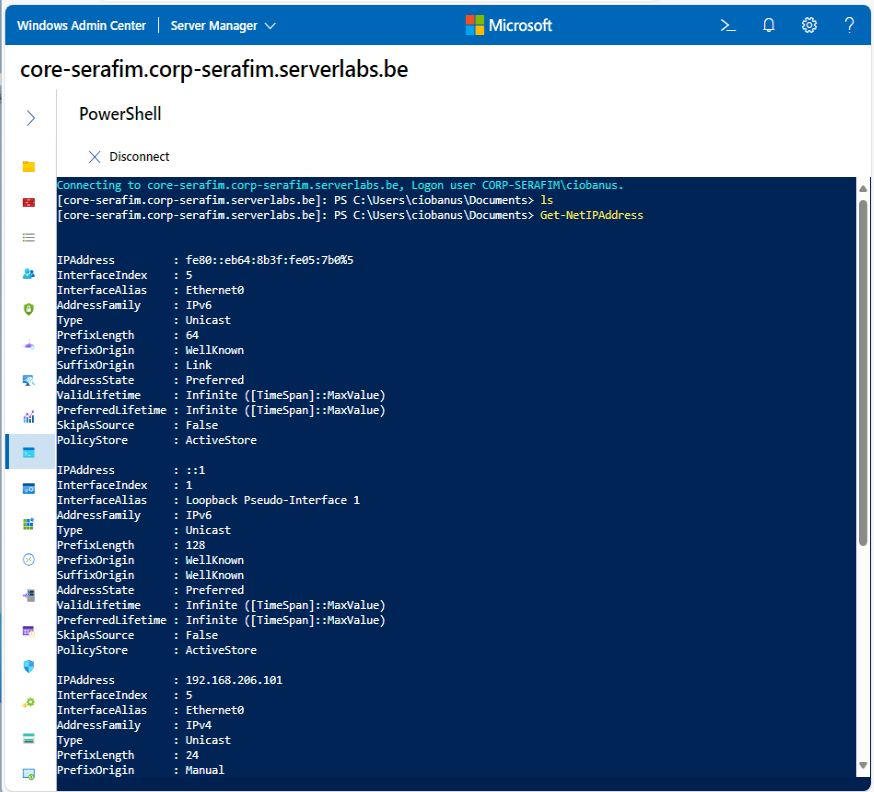
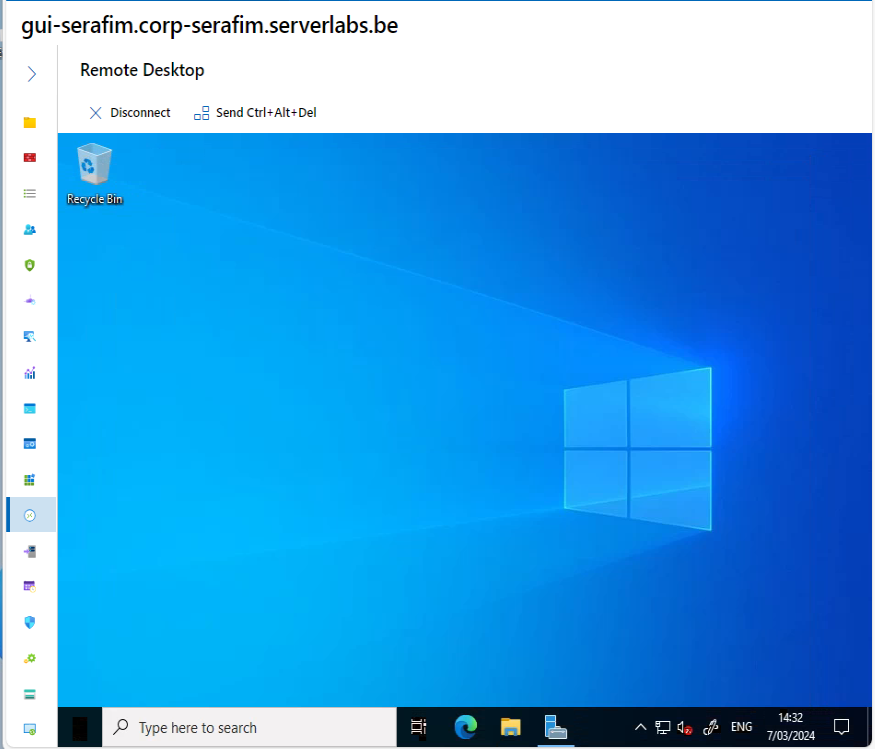


* 1. After some time, GPOs that are defined and linked in this way, will automatically be applied to all relevant devices in the domain, but this may sometimes take a few hours. To speed this process up, open a commandline window and run the “gpupdate /force” command. A restart of the VMs may also be needed.

1. Now check that the GPO was effectively applied by connecting to the VMs through remote desktop and/or by checking the remote desktop settings for all machines in Windows Admin Center.



Looks like it got activated



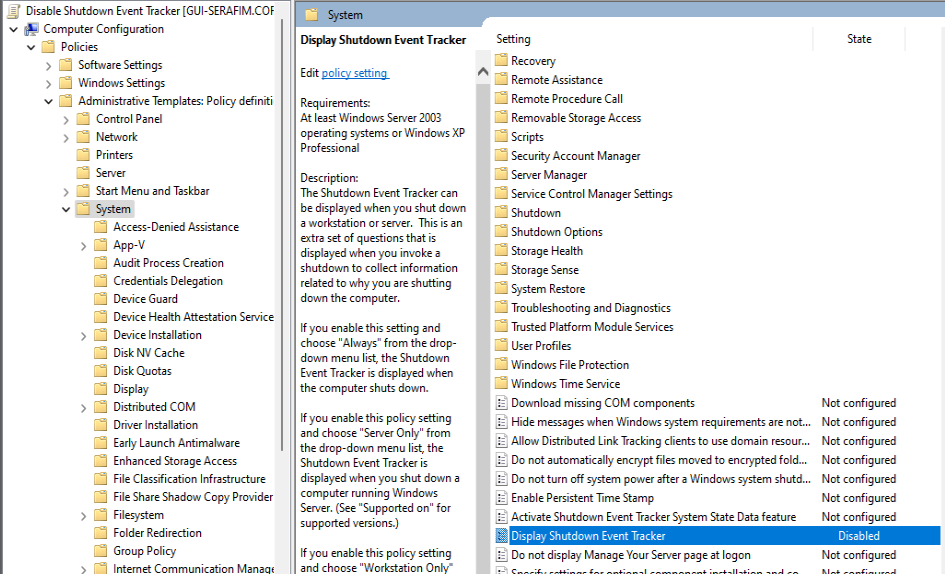
For the 2 I could connect to the desktop via WAC. But for Win 11 I tried to execute a remote command, but it would not work, so I tried Remote Desktop Services. I checked the Lab 3, and apparently there I also could only run the commands on servers, but not on the Win 11

## Fun with GPOs – Defining some new policies

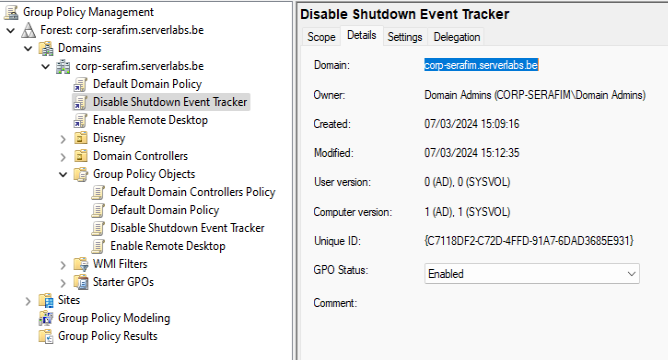
1. If you shut down a Windows server machine, it will by default ask you a reason for the shutdown. Create a **new GPO** in the GPMC app called **”Disable Shutdown Event** **Tracker“** to disable these settings for every computer in your domain.

Tip: Make use of the search function in the *spreadsheet* WindowsPolicySettings.xlsx (cfr Leho) to find the applicable policy.

Paste below a screenshot of the policy setting you changed for this.



Now check the status of your new GPO in the GPMC app (right-click the new GPO) and paste below a screenshot of the content of its *Details* tab.

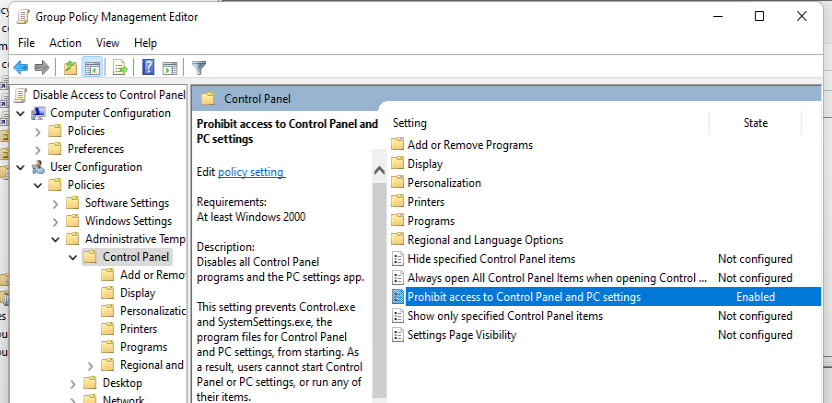


I do not know if I had to link it, but I linked it, as it is probably needed to start working.

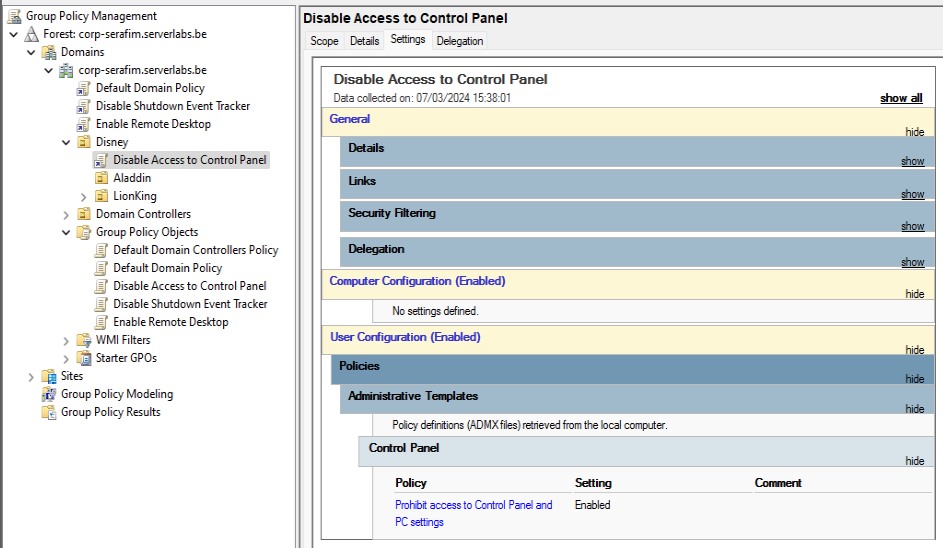
Check that your new GPO is working by restarting your GUI server. Normally, no question should be asked when shutting down that server.

First, I had to use `gpupdate /force`, and then I restarted the server once, and on the second restart – it did not ask for anything else

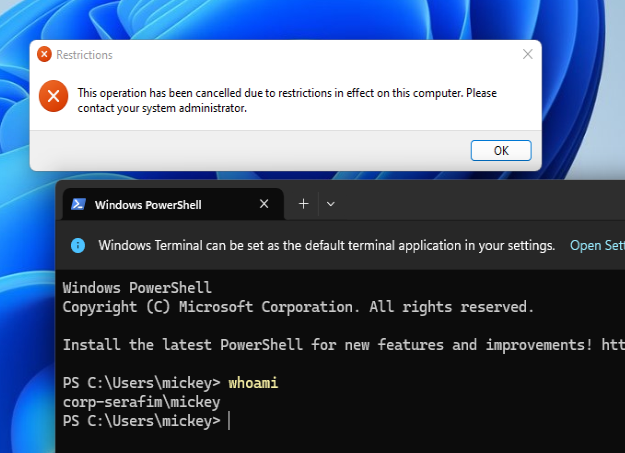
1. Using the GPMC app, create a new GPO called **”Disable Access to Control Panel“** to make sure that Disney users (only those users!) no longer have access to the Control Panel. Do not use filters!



Paste below a screenshot of the contents of your GPMC app with the linked new GPO in the left pane and in the right pane the contents of the Settings tab where the recently set policy is clearly visible.



Sign in with a Disney user account on your Win11-VM and try to open the Control Panel. Paste below a screenshot of the error message you see.



Also try to open the Settings app. What happens now?

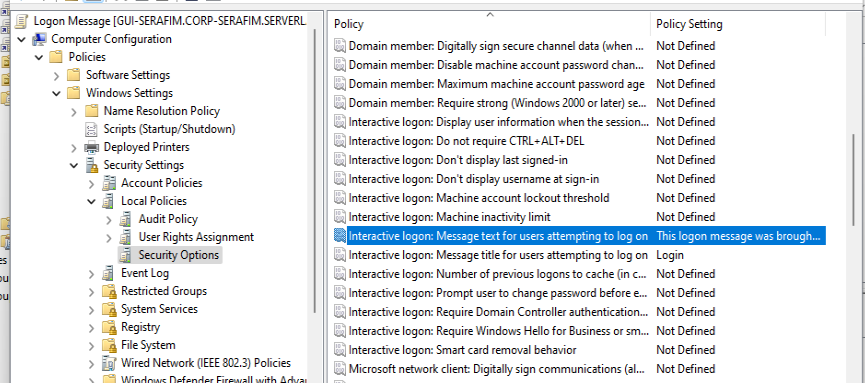
It tries to open it, then fails, and then retries again

1. Now log in to your Win11-VM with your personal domain user account again.
2. Using the GPMC app, create a new GPO called **”Logon Message“** to display an "interactive logon message" on the screen. Such a message is displayed when a user presses the Ctrl-Alt-Del keyboard combination to log in.

You will need to configure 2 policies for this:

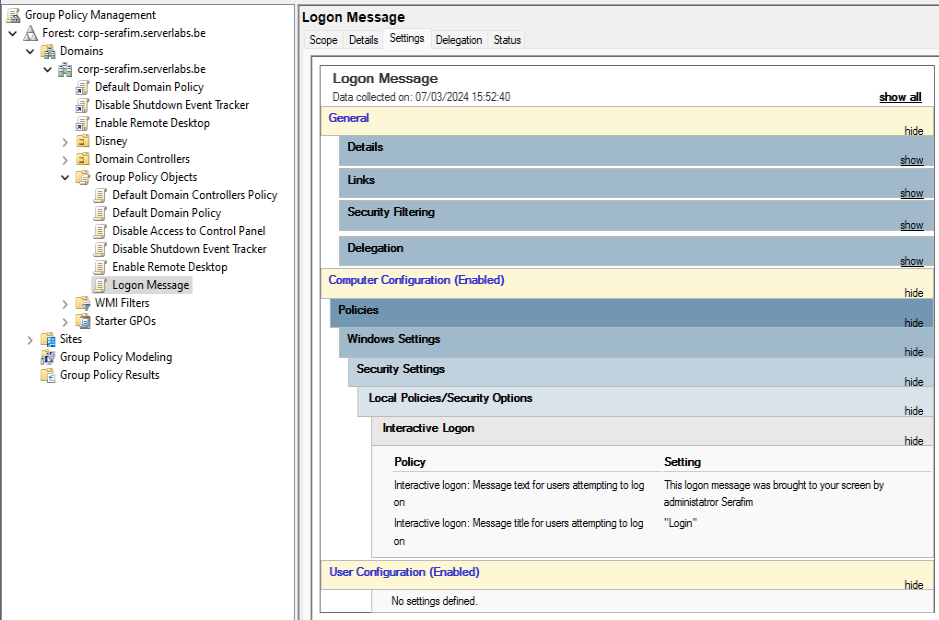
* A Title for the Message
* The content of that message

Choose the following text as the content of that message:

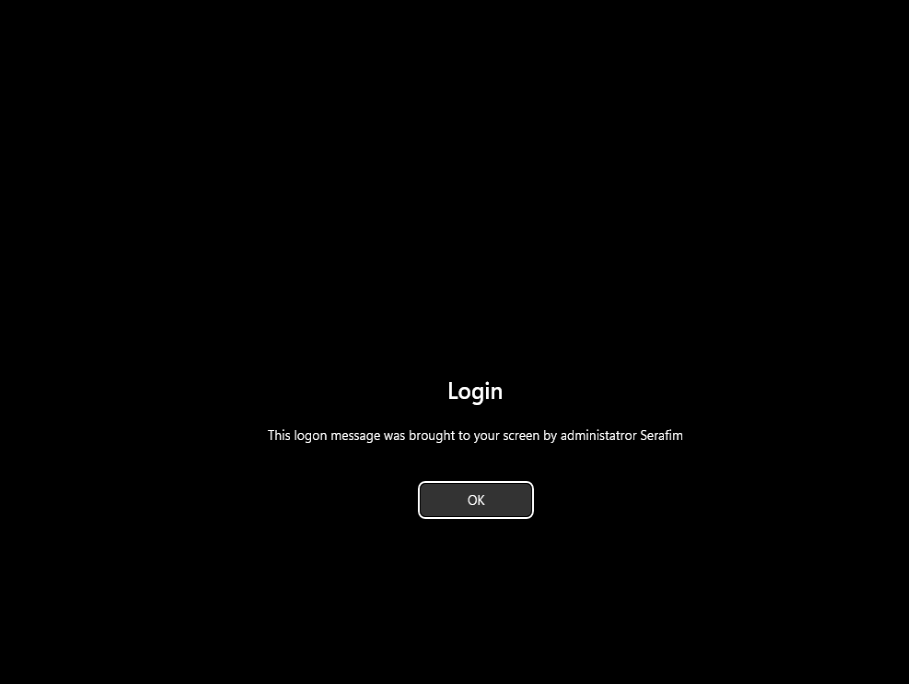
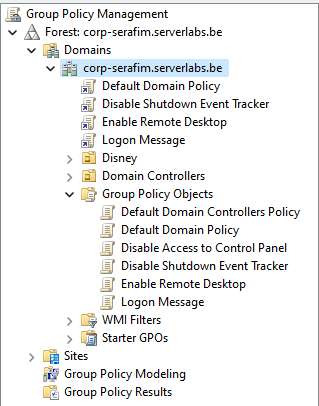


“This logon message was brought to your screen by administatror <your name>”.

Paste below a screenshot of the Settings tab of the GPO.



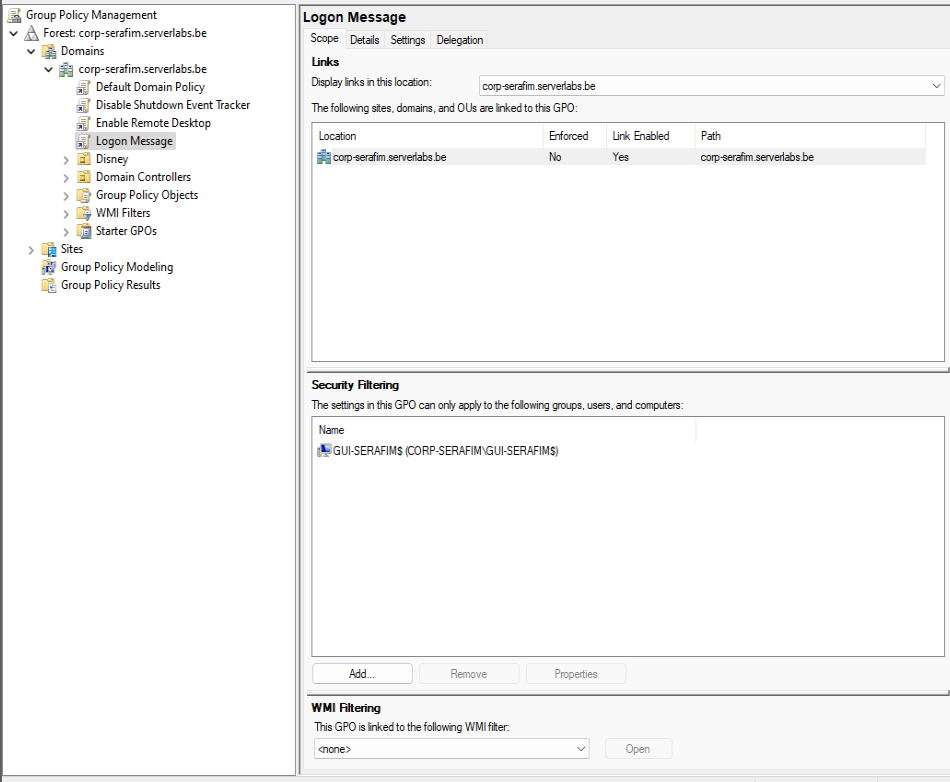
Link this GPO to your **entire domain**.This will show the message on every computer in your domain when pressing the Ctrl-Alt-Del key combination for login. Test this by restarting your Win11-VM and signing in with your personal domain user account.



1. Use **security filtering** in the GPMC app to ensure that this message is only displayed on your GUI server.

Tip: Security filtering of a specific GPO can be found in its “scope” tab.

Paste below a screenshot of the pane in which your entered security filter can be found.

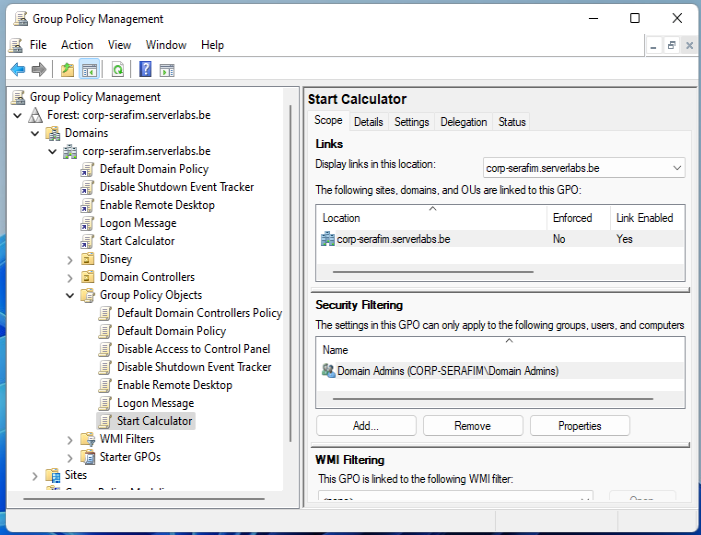
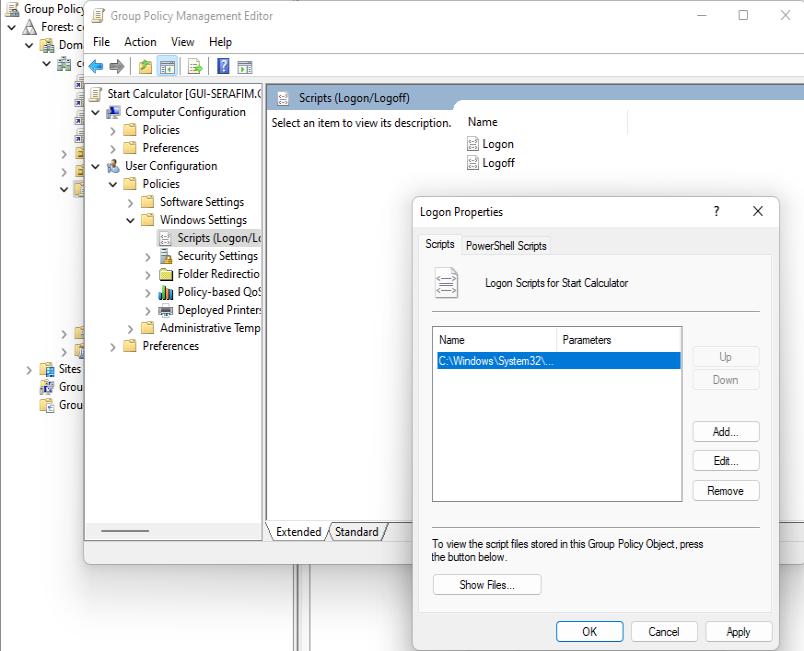


I deleted the Authenticated Users, and changed it only to a computer, and now it works.

Check that this filter works by (re)booting your GUI server and your Windows 11 VM. Normally you should only see the message on your GUI server...

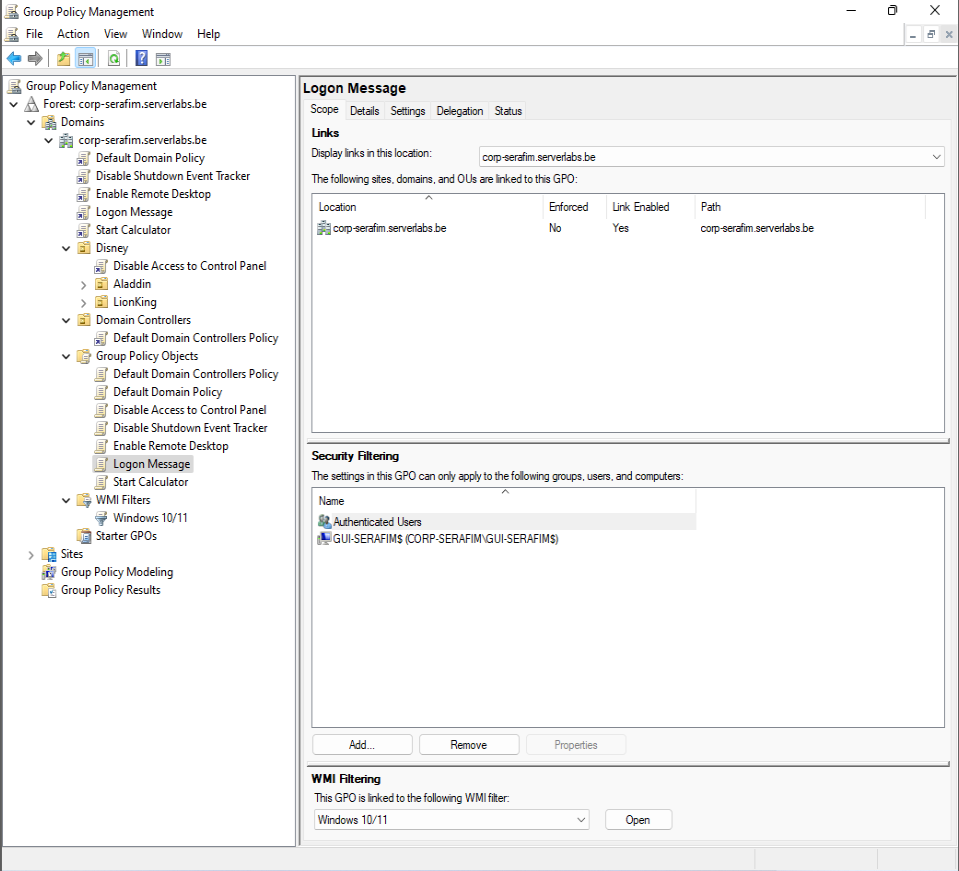
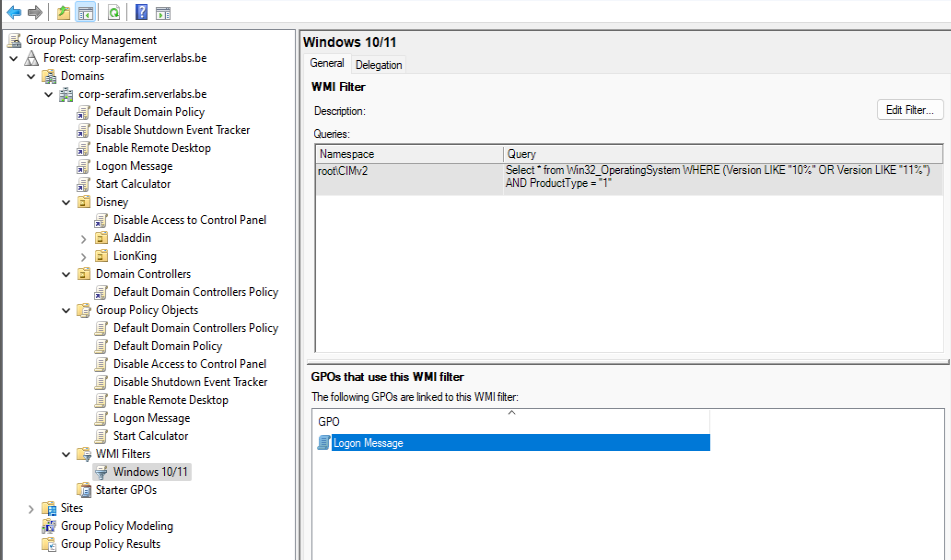
1. Create new GPO called “Start Calculator” that runs the Windows Calculator (calc.exe) when domain administrators log into a machine.

Now Change the GPO you created in such a way that the logon message will only be displayed on Windows 10/11 clients (so NOT on any of the servers). For this you will have to use a “dynamic” filter.



**Tip**: First create a suitable **WMI filter** (search for information on the Internet) and then connect this filter to your GPO.

Paste below a screenshot of your used WMI filter.



Instructions are a bit unclear for me, as I am creating a GPO for calculator, but am I supposed to link it to the whole domain? or only the domain administrators and where do I edit that?

And for the Logon Message, do I get rid of the GUI-SERAFIM specification, and leave only authenticated users?

Don't forget to test this GPO! Now the logon message should only be shown on your Win11-VM.

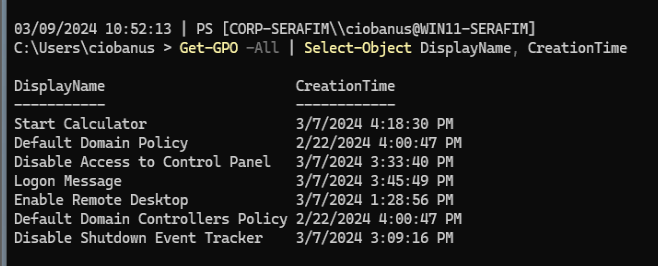
The Logon Message is only shown on the Win 11 machine, but the calculators start on every machine. I logged in with my domain administrator, and my local domain administrator (own account)

Additionally, this calculators bug out, and do not appear all the time. I tried to restart my Win 11 sometimes, and it would show the logon message, but not the calculator (not always shown). So this is still a question, because the user I login with – is a domain admin

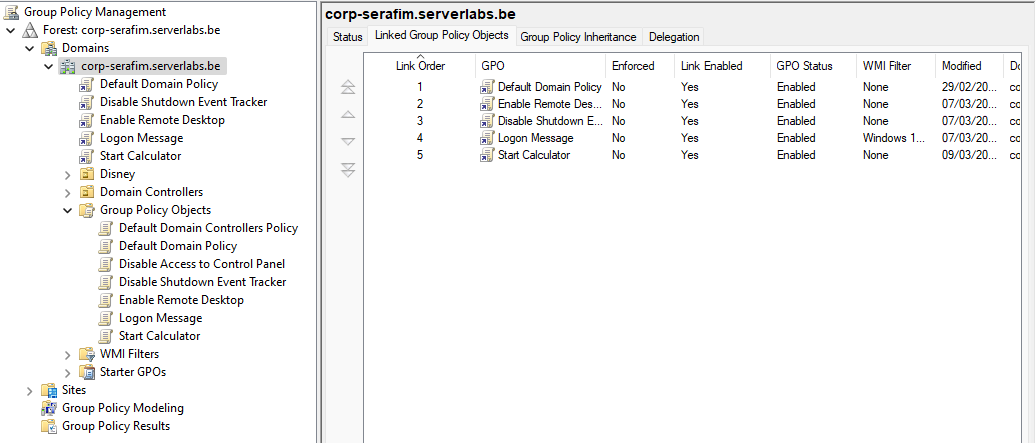
## GPO Inheritance and Precedence – When do specific GPOs apply?

1. In the previous questions, we’ve created a number of GPOs that apply to (subsets of) the domain. Now show all the GPOs in the domain by using a PS-cmdlet. Restrict the output of your cmdlet to the name of the GPO and the date it was created. Paste a screenshot of your cmdlet and its output here.

Get-GPO -All | Select-Object DisplayName, CreationTime



1. Now go back to the GPMC app and click on your domain name. A number of different GPOs should now be linked to your domain. Because each GPO can contain multiple policies, it is possible that conflicting policy settings are defined in the different GPOs. How can we know what GPO gets precedence in such a case? For this, we’ll use GPO priority and link order.  
     
   GPO settings with a low priority will always be executed first, followed by GPO settings that have a higher priority. This ensures that high-priority GPO’s will always override lower-priority GPO settings in the case of conflicting settings.



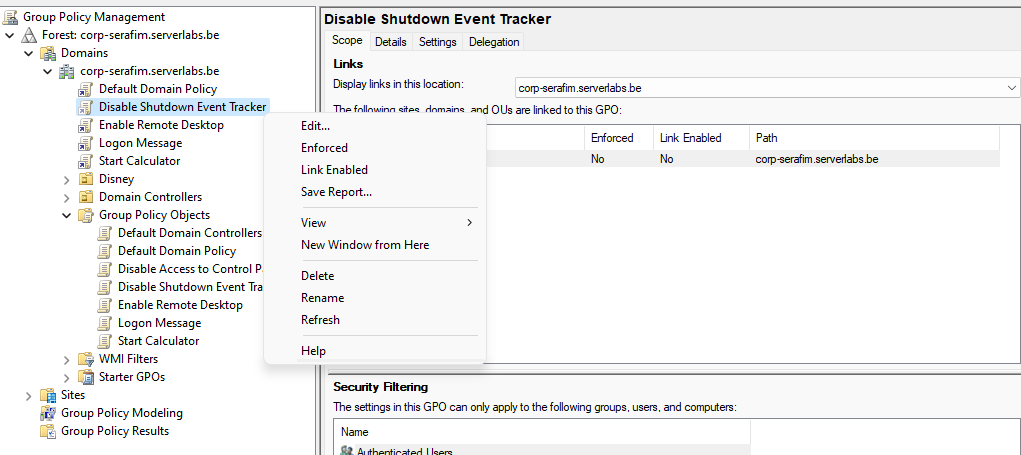
In the right pane, click on the tab “Linked Group Policy Objects” to view the priority order of the GPO’s. Which GPO is last applied and thus has the highest priority: the one with the lowest or the one with the highest “link order”?

The highest priority (5) is for the “Start Calculator”, and it will most probably be the one to be applied lastly

Note that in this window it is possible to change the priorities by using the up and down arrow keys. Do NOT do this.

1. Using the Group policy management app, disconnect the GPO called **”Disable Shutdown Event Tracker“**, without removing the GPO link in the console.

Right-click > Link Enabled

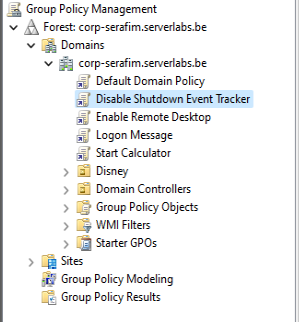
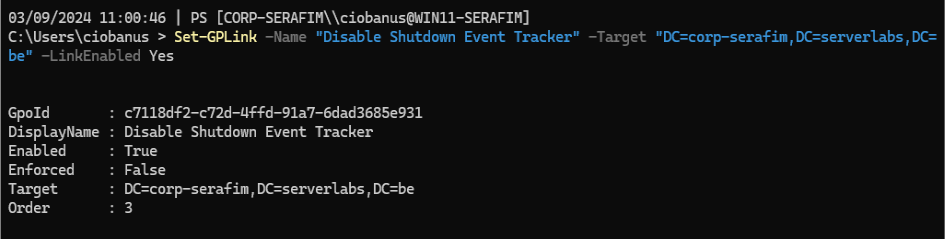


How does the console indicate that the link is disconnected?

It greyed out the little arrow next to it.

Now reconnect this GPO to the domain by using a PS-cmdlet. Paste a screenshot of your cmdlet and its output here.

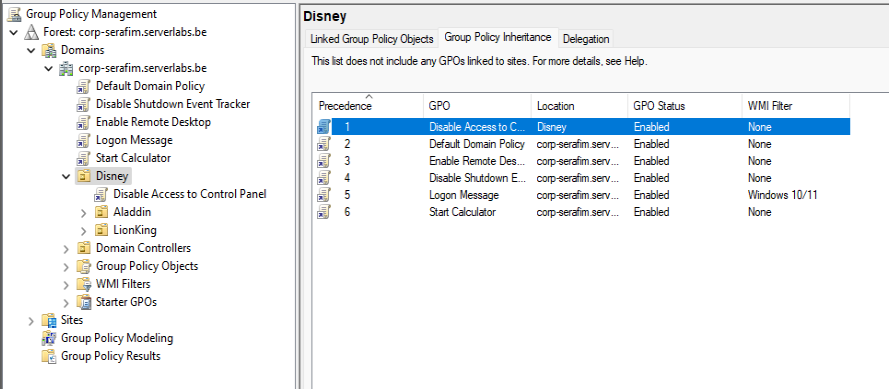
Set-GPLink -Name "Disable Shutdown Event Tracker" -Target "DC=corp-serafim,DC=serverlabs,DC=be" -LinkEnabled Yes



1. GPOs can be linked to a “container” (a domain or OU) in two ways: Either explicitly or implicitly through inheritance from a parent container. Note below the names of the GPOs that are explicitly and implicitly linked to the “Disney” OU.

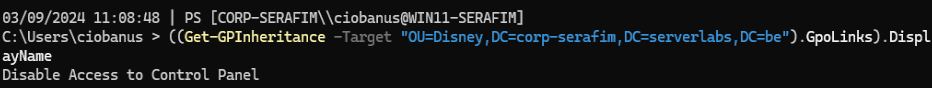
**Explicitly linked GPOs =** Disable Access to Control Panel

**Implicitly linked GPOs =** Default Domain Policy, Enable Remote Desktop, Disable Shutdown Event Tracker, Logon Message, Start Calculator

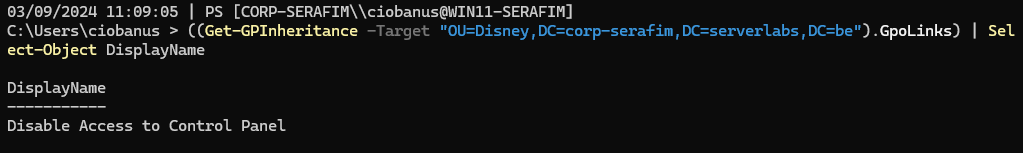


With a PS-cmdlet, show the names of the GPOs (and no more than that) that are explicitly linked to the **Disney**-OU.Paste below a screenshot of your cmdlet and its output.

((Get-GPInheritance -Target "OU=Disney,DC=corp-serafim,DC=serverlabs,DC=be").GpoLinks).DisplayName

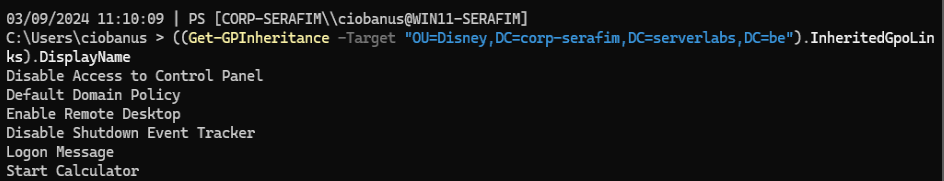


((Get-GPInheritance -Target "OU=Disney,DC=corp-serafim,DC=serverlabs,DC=be").GpoLinks) | Select-Object DisplayNam

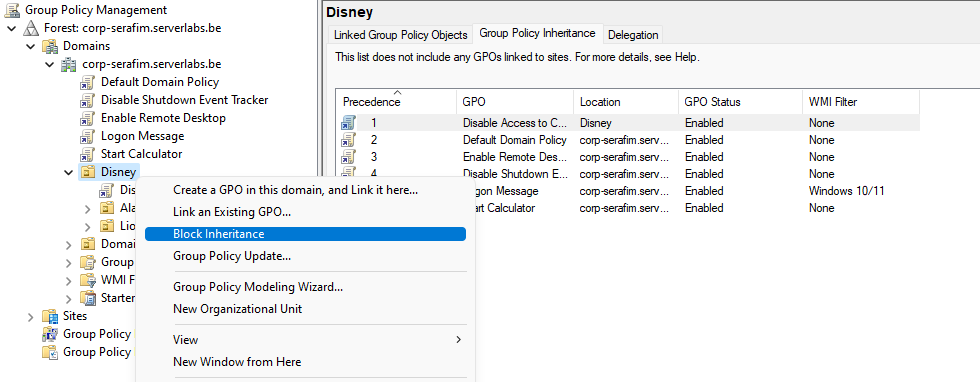


With a PS-cmdlet, show the names of the GPOs (and no more than that) that are explicitly and implicitly linked to the **Disney**-OU. Paste below a screenshot of your cmdlet and its output.

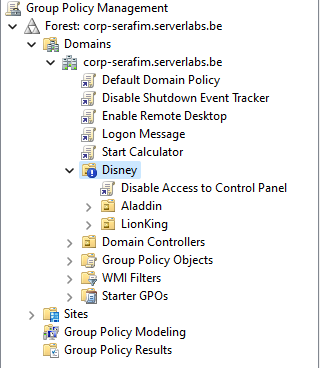
((Get-GPInheritance -Target "OU=Disney,DC=corp-serafim,DC=serverlabs,DC=be").InheritedGpoLinks).DisplayName



1. By default, a container implicitly links to the GPOs that are already explicitly or implicitly linked to its parent container. However, you can block this GPO inheritance for a specific container. Apply this to the “Disney” OU using the GPMC app.



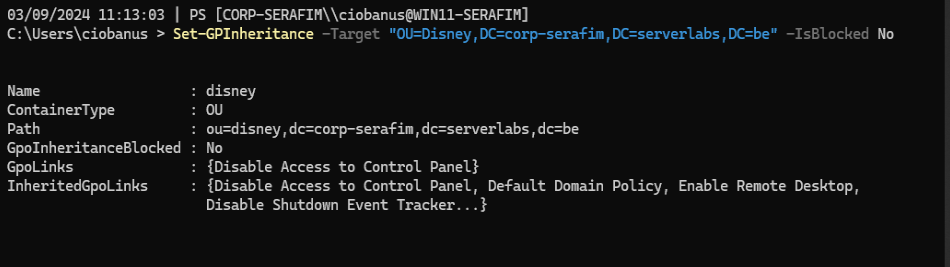
How is this indicated in the GPMC app?



With a small exclamation mark

Now re-enable GPO inheritance for the Disney OU by using a PS-cmdlet. Paste a screenshot of your cmdlet and its output below.

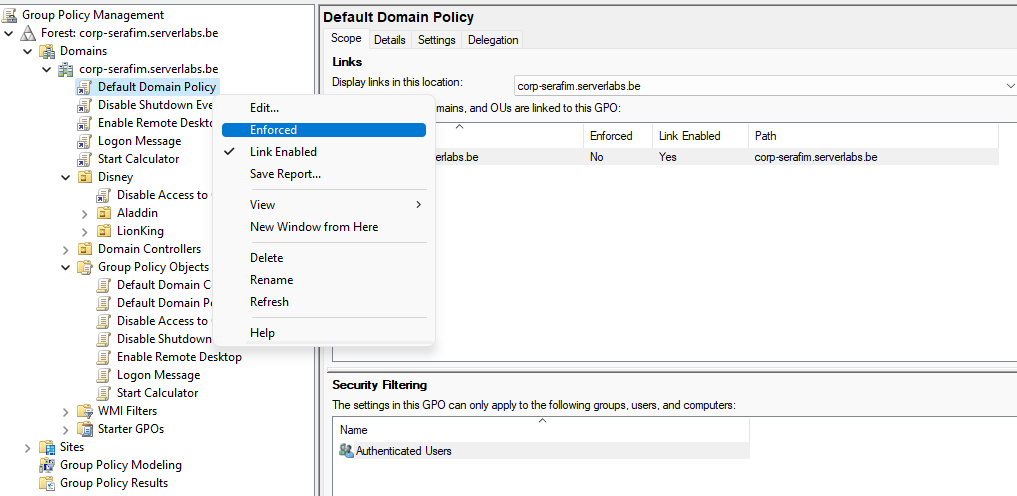
Set-GPInheritance -Target "OU=Disney,DC=corp-serafim,DC=serverlabs,DC=be" -IsBlocked No



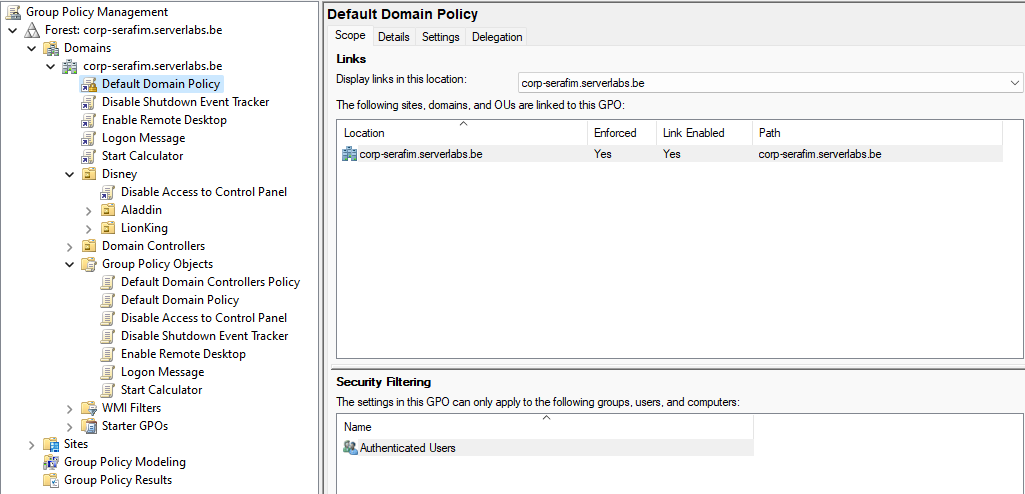
Then check that GPO inheritance is effectively re-enabled in the GPMC app (don't forget to refresh).



1. If a container is both implicitly and explicitly linked to GPOs, it again may happen that the objects in that container have conflicting settings. In this case the settings defined in the explicit GPOs will get precedence. However, you may deviate from this standard behavior by forcing the settings in an implicitly linked GPO. Test this out by imposing the “Default Domain Policy” in the GPMC app.



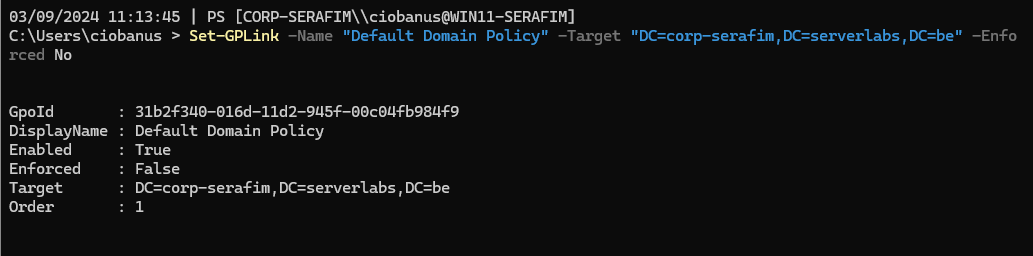
How is this indicated in the GPMC app?



With a small lock

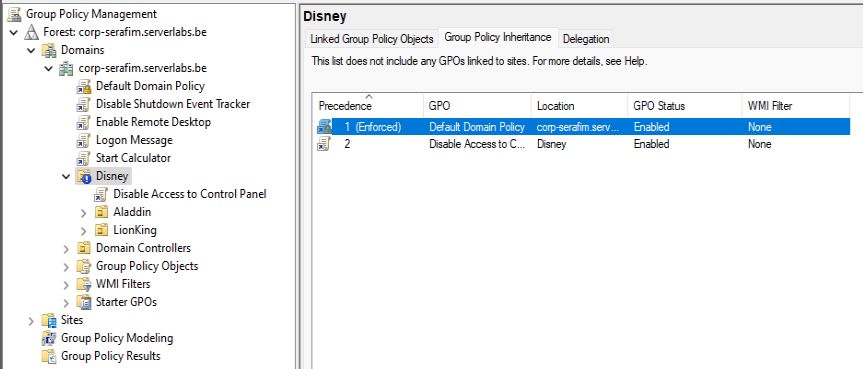
Now disable this setting again, but this time using a PS-cmdlet. Paste below a screenshot of your cmdlet and its output.

Set-GPLink -Name "Default Domain Policy" -Target "DC=corp-serafim,DC=serverlabs,DC=be" -Enforced No



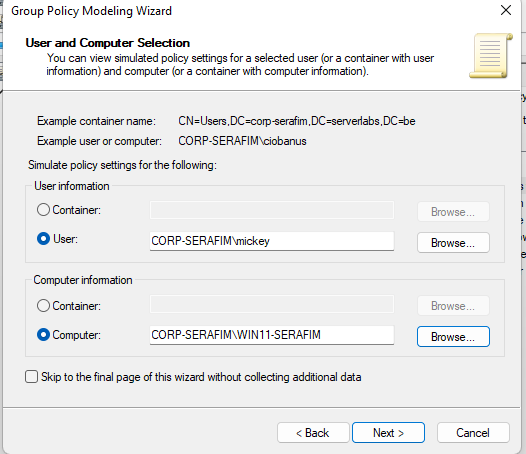
Can a “forced” GPO be blocked by applying “Block Inheritance” to an OU?

Nope, it will still be applied, because it is forced.

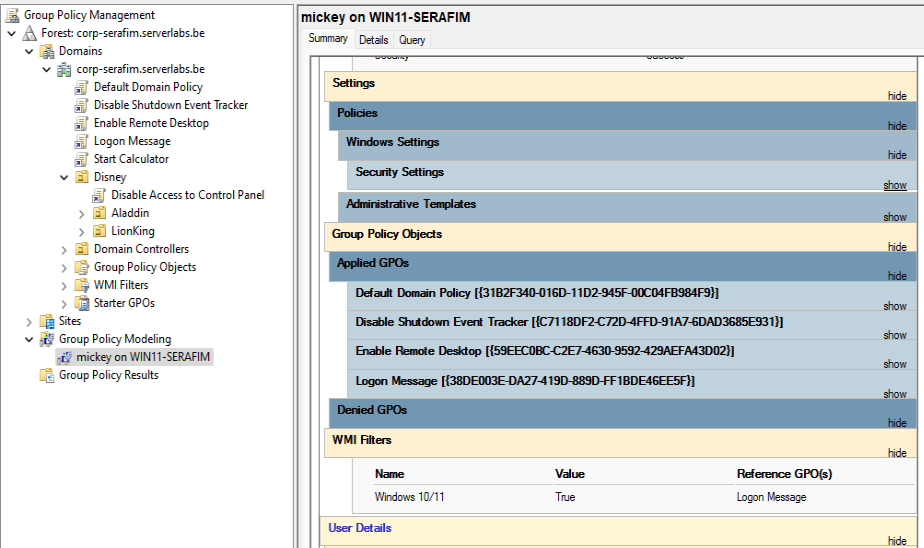


## Policy simulation – making sure that the right policies apply!

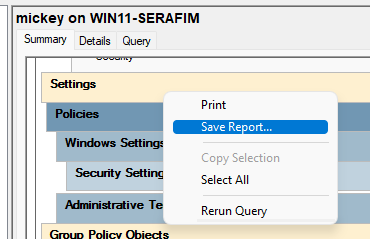
1. As we’ve seen throughout the lab, multiple GPOs can apply at the same time, and their policies have to be combined using a (sometimes complex) set of rules for precedence and inheritance. Fortunately, the GPMC app can also be used to create simulations of policies that would be applied to a particular user if they log in to a specific computer. In the GPM app, use the “Group Policy Modeling” wizard to find out which group policy settings (of all GPOs) would effectively apply if user **mickey** signed in to your **Win11-VM**.



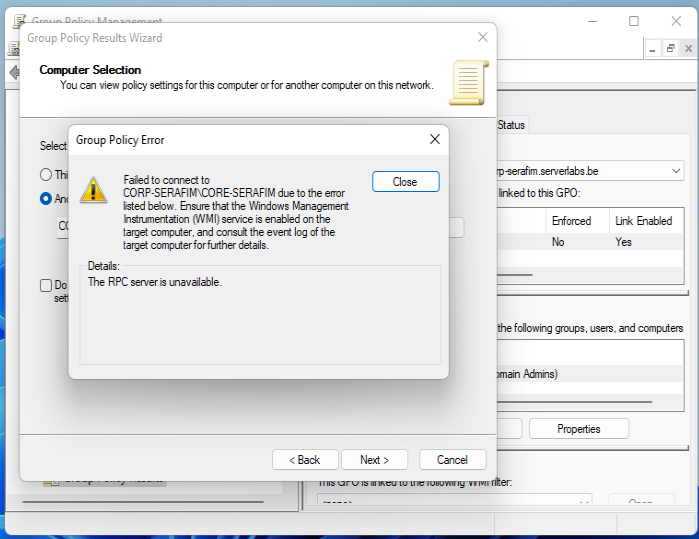
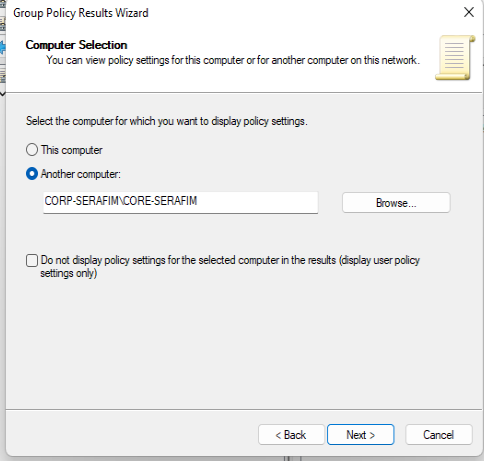
After going through the wizard, you will see in the right pane a detailed overview of which policies apply when the selected user logs in to the selected computer.



Use the GPMC app to create a HTML-formatted report of these policies **and upload this report to Leho.**



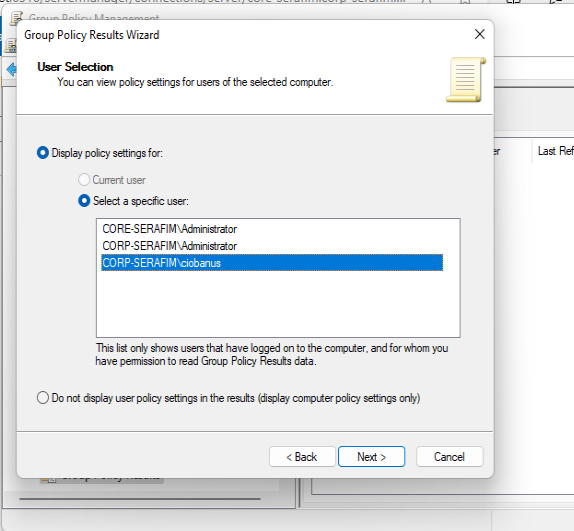
1. In the GPMC app, you can also make simulations of policies for a particular user on a specific computer using the “Group Policy Results” wizard, provided that the user has already logged in to that computer. Use that wizard to do a simulation for your personal domain user account on your core server.



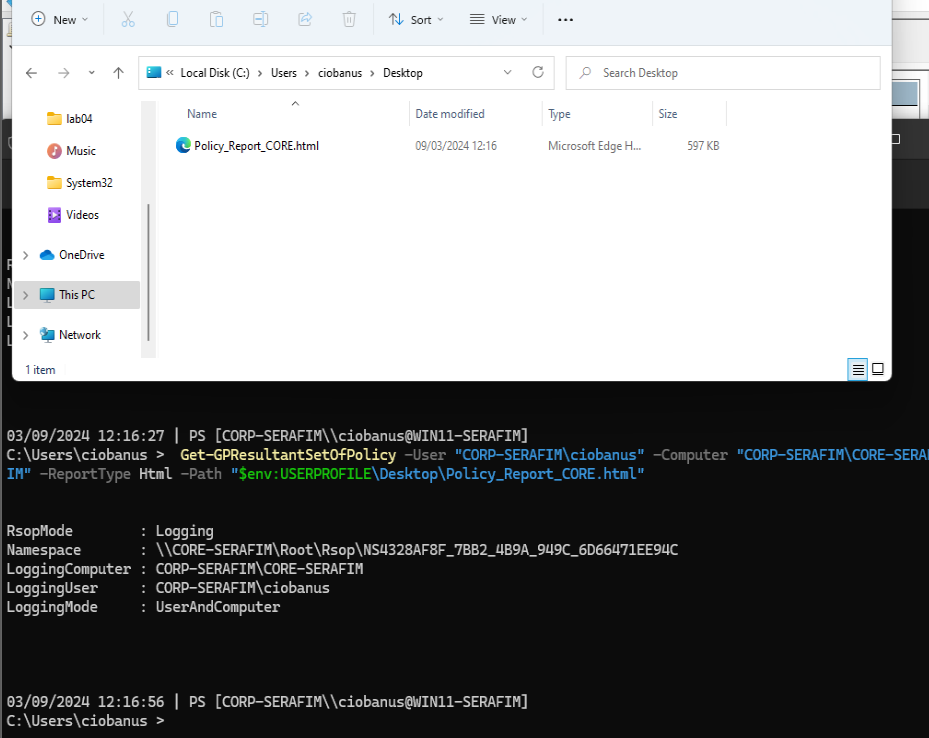
Looks like a firewall issue on my core server, as disabling it fully – solves the issue

Yes, it was a firewall issue, becuase other processes were perfectly running on the system.

The firwall rule was (Inbound) Windows Management Instrumentation (WMI-In), by enabling it, I can continue with the assignment.



1. Use a PowerShell-cmdlet to create a HTML report of the policy settings from the previous command and save it on the Desktop of your local profile folder.



Get-GPResultantSetOfPolicy -User "CORP-SERAFIM\ciobanus" -Computer "CORP-SERAFIM\CORE-SERAFIM" -ReportType Html -Path "$env:USERPROFILE\Desktop\Policy\_Report\_CORE.html"

1. the “default” profile is needed here specifically for the GUI server. While the network connections of the Win11 and Core server connections are considered Domain connections, the network connection of the GUI server is not, because it links to a non-domain DNS server (the VMware DNS) through this connection. In the firewall, the GUI server’s connection will be considered to be “public” or “private”, depending on previous configurations (to check this, compare the “NetworkCategory” properties for the different VMs in the Get-NetConnectionProfile cmdlet). [↑](#footnote-ref-3)