Lab 14:

Windows Auditing

Windows Server Security  
 2024-2025

© Daan Pareit

## Introduction

# Lab concept

In this lab we’ll explore how to audit/log security related events and file access on Windows workstations and servers.



# Learning goals

* Audit settings in Policy Editor
* File access auditing
* Auditing in an Active Directory

# Practicalities and prerequisites

You’ll need:

* Your Windows 11 client VM
* Your Windows Server 2025 VM (“KING”)

## Auditing Logins

* Login to your Windows Client (‘DESKTOP-XXXXXXX’) with your local admin account ‘Mickey Mouse’.

.\Mickey Mouse

* Open Security Settings (gpedit.msc or secpol.msc) . Go to “Local Policies > Audit Policy”.

A screenshot of a computer

Description automatically generated

* There are two policies regarding “logon events”. Which policy audits each instance of a user attempting to log on to or to log off to **this** specific computer?

A screenshot of a computer

Description automatically generated

Audit logon events, which literally says – “to **this** computer”

* What is its current setting? Have a closer look in the ‘Explain’ tab. What are the default fallbacks for auditing logon and logoff?

A screenshot of a computer

Description automatically generated

* However, Windows is no longer following these “category” settings but applies newer “subcategory” settings. Have a look at “Advanced Audit Policy Configuration > System Audit Policies”. In the description it refers to another policy setting. Which one?

A black text on a white background

Description automatically generated

Local Policies\Security Options, or the Audit: Force audit policy subcategory settings.

Have a look at that one. How is it configured? What is the default fallback?

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Enabled by default.

To allow audit policy to be managed using subcategories without requiring a change to Group Policy, there is a new registry value in Windows Vista and later versions, SCENoApplyLegacyAuditPolicy, which prevents the application of category-level audit policy from Group Policy and from the Local Security Policy administrative tool.

By default it probably has some default values in which it decides to apply different categories or not.

* Thus, we need to have a look at “Security Settings > Advanced Audit Policy Configuration > System Audit Policies” instead to find the policy for logon. How is it configured and what is the default fallback? And for logoff?

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The **Logon** is not configured by default but can be. The default fallback is to only Log Success for Clients, and Success + Failure for Servers.

A screenshot of a computer

Description automatically generated

A screenshot of a computer security system

Description automatically generated

Default fallback is for successful logoffs

* We noticed that there’s some discrepancy in the descriptions in the ‘Explain’ tabs and actual audit event logs. To verify what is now actually being audited, you can run the “auditpol” command at the terminal (run as admin). Find the appropriate options, via “auditpol /?” to figure out what is actually being logged for logon/logoff.

auditpol /?

auditpol /get /?

auditpol /get /category:\*

A screen shot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

* Now locate the event logs. You should see audit events for users successfully logging on and off to the computer. What is the event ID for a successful logon? And for a successful logoff?

To view this: Go to Event Viewer - > Windows Logs -> Security

A close-up of a computer

Description automatically generated

Logon Success: 4624 (ID)

A close-up of a computer

Description automatically generated

Logoff Success: 4634 (ID)

* Log out and try to first type the wrong password to have a failed login. Now go to the event logs again. What is the event ID for a failed logon?

It is very strange to me that I do not actually see a Failed Logon event, without touching anything really.

To fix this, I enabled to log both Success and Failure in the previous policies.

A screenshot of a computer

Description automatically generated

The ID is 4625

I saw some previous logs with the “Lock” emoji, and I understood my fault. I went to disable the setting I enabled, and now the logs do not appear at all. I do not get it.

I went to check my auditpol command, and now it says that NOTHING IS BEING AUDITED. WINDOWS JUST SAID FINE I WILL JUST TURN EVERYTHING OFF BECAUSE YOU TOUCHED 1 POLICY!!!

Went back to a snapshot of mine, and saw the logs

A screenshot of a computer

Description automatically generated

* To only view these events, you can use the filter in the side panel. You can also use PowerShell and the cmdlet:

Get-EventLog -LogName Security | where {$\_.eventid -eq "<event\_id>"}

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

It works, but I guess with one event id only, in case of command.

* For the successful logon event, you’ll notice that the ‘Security ID’ and the ‘Account Name’ are not Mickey Mouse (in the ‘subject’ section). What is recorded instead? Why isn’t this ‘Mickey Mouse’ as account name? Look in the Microsoft online documentation:

<https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-logon>

A screen shot of a computer

Description automatically generated

A black background with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

This is another log though.

* What is the ‘Logon Type’ you’ll notice in the General information of the event? What does it mean?

Logon type is 2

A close-up of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

* In the event, you also find the details of Mickey Mouse as the one who was logging in. In what section (instead of the ‘subject’ section) of the event can you find Mickey’s name?

In the New Logon section? There is no other one

A computer screen shot of a computer

Description automatically generated

* Also inspect a failed logon event. Is it similar?

A close-up of a computer error

Description automatically generated

It is similar, however it gives away less information than the other one. This is probably security wise.

* What event, following a successful logon, indicates that Mickey has received extra privileges after logon? What is the name of the ‘privilege’ which indicates that Mickey has received the privilege to manage the auditing and security logs? (Look in the Microsoft online documentation again.)

A screenshot of a computer security

Description automatically generated

The name is Special Logon, the ID is 4672

The privilege that allows everything else

* Now, change the ‘Audit Logon’ policy to only log Success. (We’ll come back to this in a later exercise to see if domain policies maintain or overrule this.)

A screenshot of a computer

Description automatically generated

## Auditing the file system

Here, we’ll work locally on DESKTOP-XXXXXXX. First, specify a specify folder to be audited.

* Login with your Mickey Mouse account on the desktop.
* Create a folder ‘mytest’ on the C drive where John Doe has full access to.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

I added the User manually, but I think that was obsolete.

* Add John Doe to the SACL of that folder. Enable auditing for successful writes for him in this folder.

A screenshot of a computer

Description automatically generated

I think I did it right.

* Now, you specified SACL for a folder. But remember, importantly, you still generally allow auditing of the file system! Which policy do you need to enable for this? Do this.

A screenshot of a computer

Description automatically generated

This seems to be an option

A screenshot of a computer

Description automatically generated

Here is another one I found, afterwards, which is probably the one needed.

I ticked success there.

* Login as John Doe. Create a file in the folder.

A screenshot of a computer

Description automatically generated

* Verify this has been logged (locally). What is the event ID?

A screenshot of a computer

Description automatically generated

ID is 4658

Could not see the event because it did not save the settings for some reason.

Now we’ll use GOAA to track file system action on the entire computer.

* Enable the File System policy in GOAA category.

A screenshot of a computer

Description automatically generated

* Configure the SACL to log for file deletion by John Doe.

A screenshot of a computer

Description automatically generated

* Let John Doe create a test.txt document in its Documents folder. Then remove this file and leave Windows Explorer open.
* Switch to Mickey user without logging out John Doe.
* Look at the event viewer. What event ID indicates the file deletion?

Managed to find it only after rebooting the system. Horrible Windows.

Event ID is 4660

A screenshot of a computer

Description automatically generated

* Note that the file name is not included in the event. How can you link the event of the deletion to a specific file? Hint, again look at the Microsoft documentation for the event.

A screenshot of a computer

Description automatically generated

It depends on the “Handle ID”, and then there is the next ID is 4663 and shows the name of the file (object)

* You’ll also see what process has deleted the file, as well as its process ID. Have a look at the PID of explorer.exe process in Task Manager (for John Doe). Convert the hexadecimal value from the process id in the event log to decimal and find that this matches the process id of the Windows Explorer, still open at John Doe.

A close up of numbers

Description automatically generated

A screenshot of a computer

Description automatically generated

It matches!

* Now, disable the GOAA and File system audits again (to avoid too many logs on your VM).

## Auditing with domain policiess

Now apply auditing settings throughout a domain

* Log on to your Windows 11 VM as domain admin Donald
* Ensure that on your Windows 11 VM the following features are installed (via Settings –Apps–Optional Features):
  + RSAT: Server Manager
  + RSAT: Active Directory Domain Services and Lightweight Directory Services Tools
  + RSAT: Group Policy Management Tools Utilities

Had to install the second.

20 minutes later – Optional Features are absolutely terrible.

Add-WindowsCapability -Online -Name Rsat.ActiveDirectory.DS-LDS.Tools

Still took another 20 minutes no joke.

* Then, use the Server Manager and connect to the domain controller (KING)

Note: We’re using Server Manager now, as this is not available in Windows Admin Center yet.

A screen shot of a computer screen

Description automatically generated

* Use the ‘Active Directory Users and Computers’ tool in Server Manager. In the Active Directory, create a new Organizational Unit (OU) ‘PCs’ and put computer DESKTOP-XXXXXXX therein.

Action > New > Organizational Unit

I am not sure I only found Move that allowed me to do it.

A screenshot of a computer

Description automatically generated

* Open the Group Policy Management via Server Manager
* Create a new group policy ‘auditPCs’ and link it to your OU.

A screenshot of a computer

Description automatically generated

GPO > New > Create one

A screenshot of a computer

Description automatically generated

Link it.

A screenshot of a computer

Description automatically generated

* Edit the policy (right click the policy and choose ‘Edit’) to enable some auditing options:
  + Configure the ‘Audit Logon’: check only ‘failure’

A screenshot of a computer

Description automatically generated

* + Configure the ‘Audit File System’ but uncheck both success and failure

A screenshot of a computer

Description automatically generated

Also in the GPO: enable the “Audit: Force the usage of Advanced Audit Policy subcategories”.

A screenshot of a computer

Description automatically generated

* This policy would automatically be applied to all computers in the ‘PCs’ OU (including our Windows 11 VM) after some time or after rebooting. However, to speed things up, apply in an elevated terminal on your Windows 11 VM following command: gpupdate /force
* Generate reports in ‘Group Policy Results’ in the Group Policy Management via the wizard for your Windows 11 VM for the (non-domain) user ‘Mickey Mouse’.

A screenshot of a computer policy

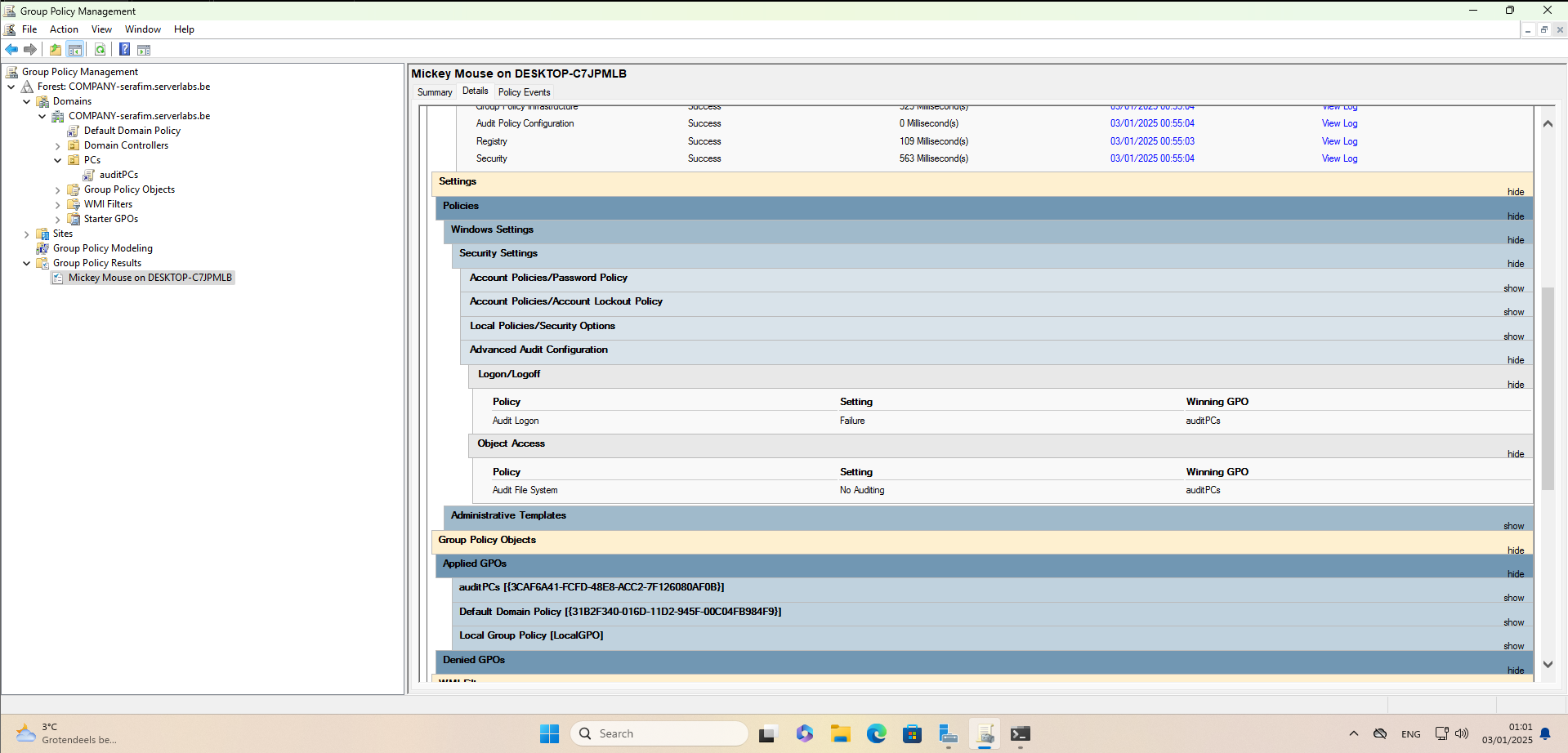
Description automatically generated

* In the report, go to Computer Details > Settings > Policies > … to view the resulting audit policies and ‘winning GPOs’. In previous exercises we’ve applied some audit settings locally and some in the domain. Which one is winning for the different settings?

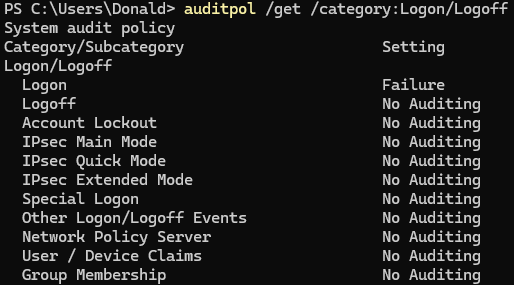
A screenshot of a computer

Description automatically generated

GPOs seem to be the most powerful ones, because it like applies to a whole domain, and not only local on one computer.



* Note: Using ‘auditpol’ and appropriate options as before also shows this merged local and domain policies



A screen shot of a computer

Description automatically generated

Just reminding that in one of the questions before this we actually disabled the other policies.

## Resources

* <https://docs.microsoft.com/en-us/windows/device-security/auditing/security-auditing-overview>
* Windows Group Policy Troubleshooting A Best Practice Guide for Managing Users and PCs Through Group Policy, Apress, 2016
* Security Auditing, <https://docs.microsoft.com/en-us/windows/device-security/auditing/security-auditing-overview>
* <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/>[advanced-security-auditing-faq](https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-auditing-faq)