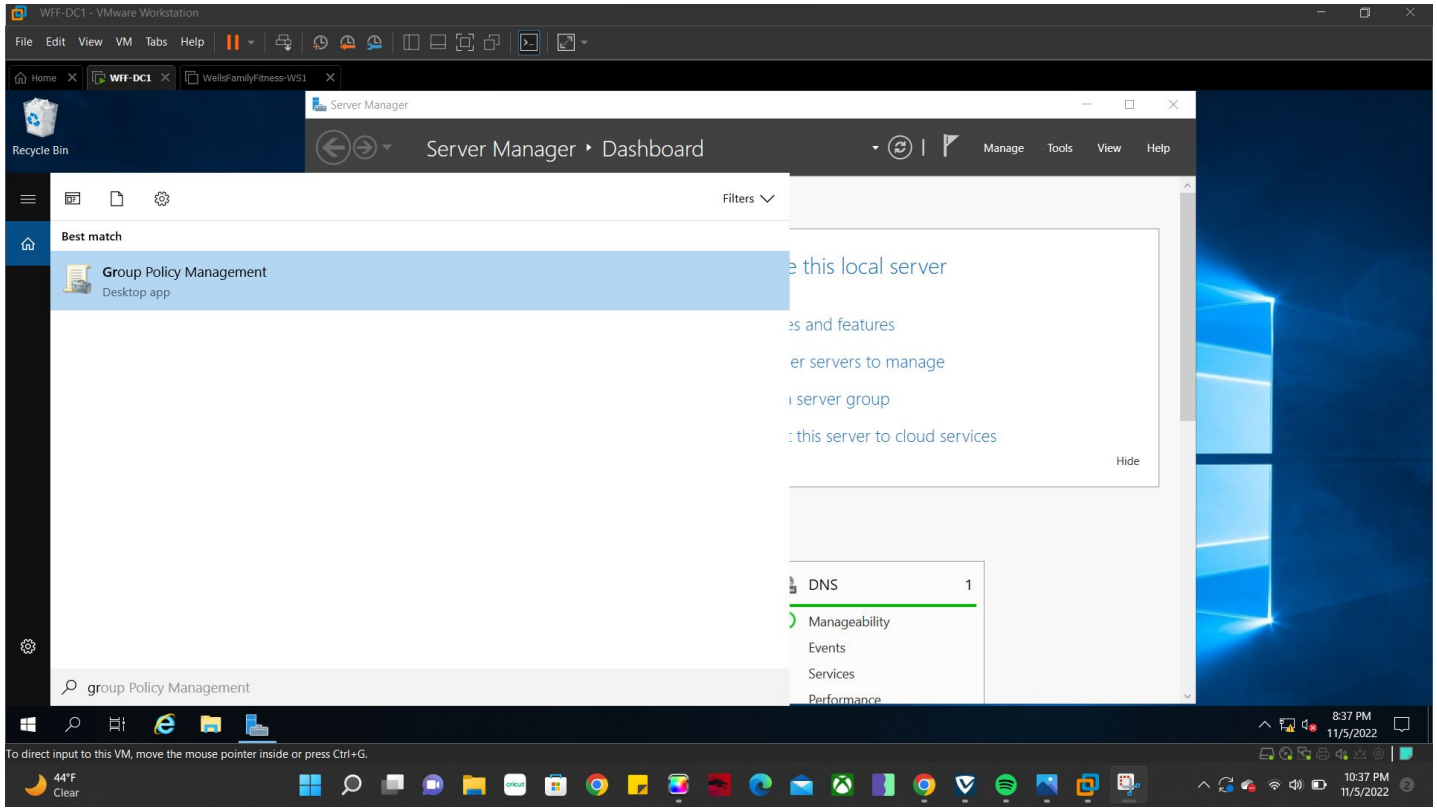
1. In the DC server open Group Policy Management as Administrator

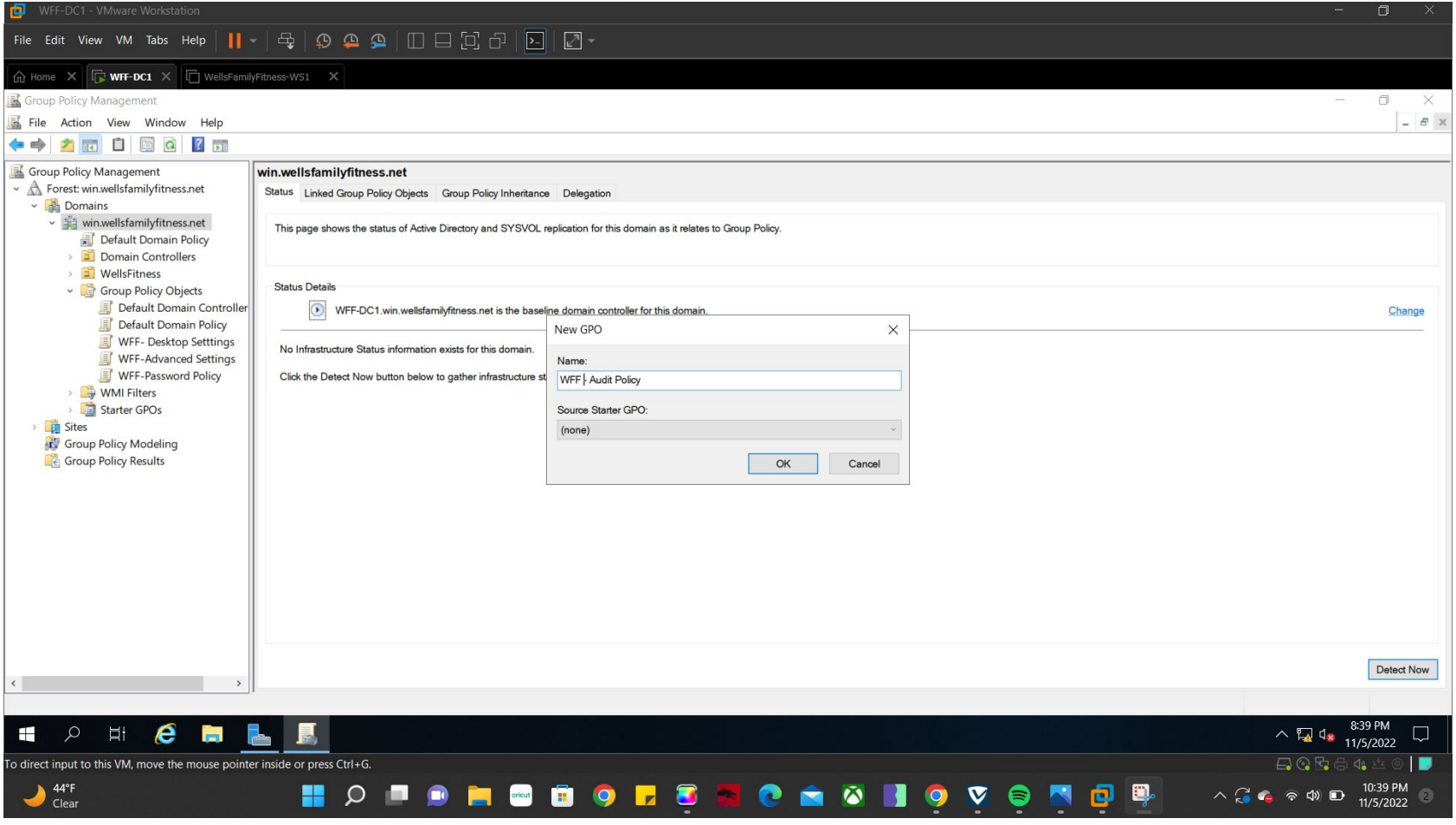


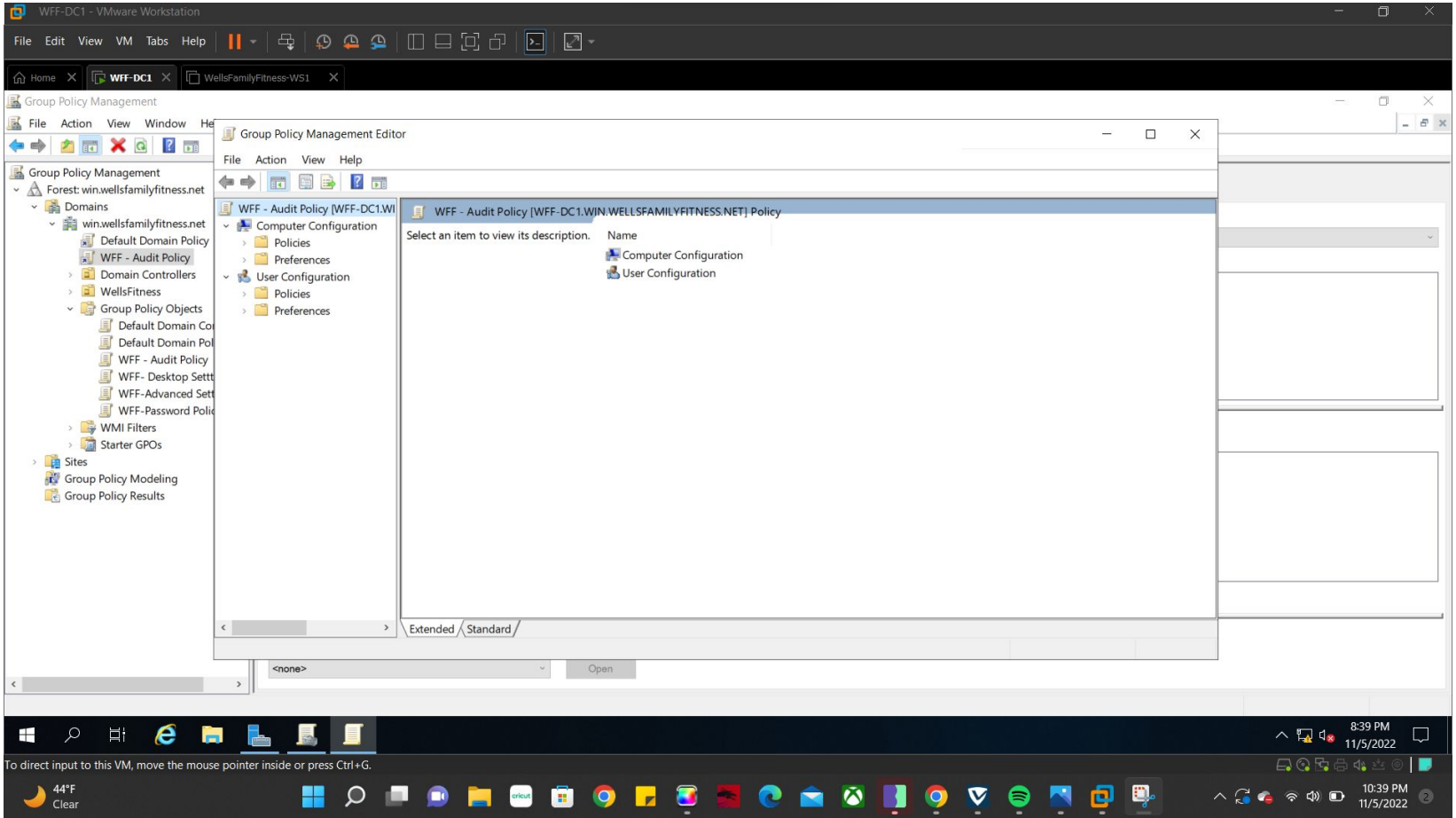
AUDITING COMMON THREATS ON VMWARE-WINDOWS SERVER 2016

ITT-121- System Administration and Maintenance

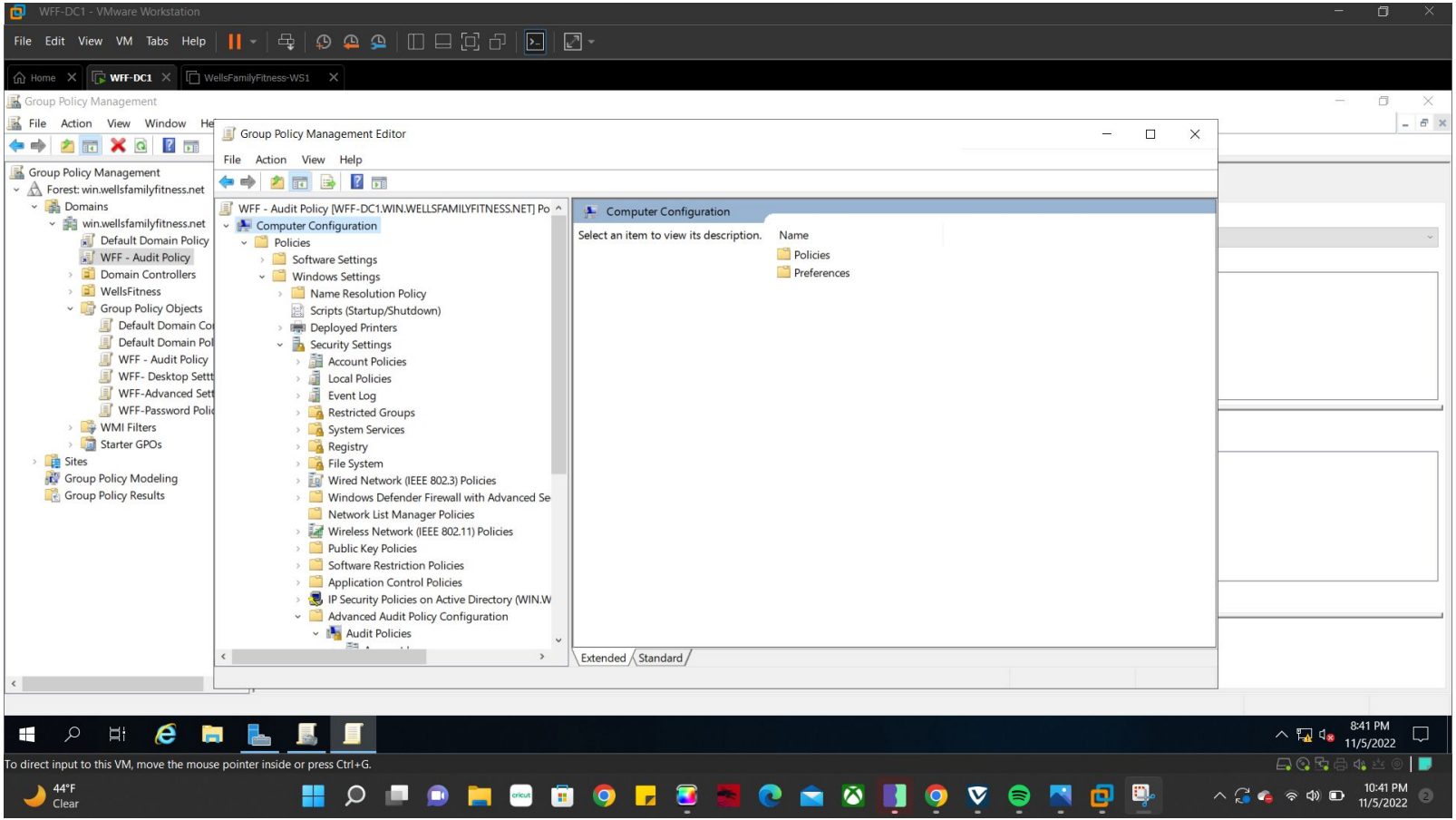
Liela Pressley

2. Under the domain of your corporation create a new group policy and label it NAME- Audit Policy

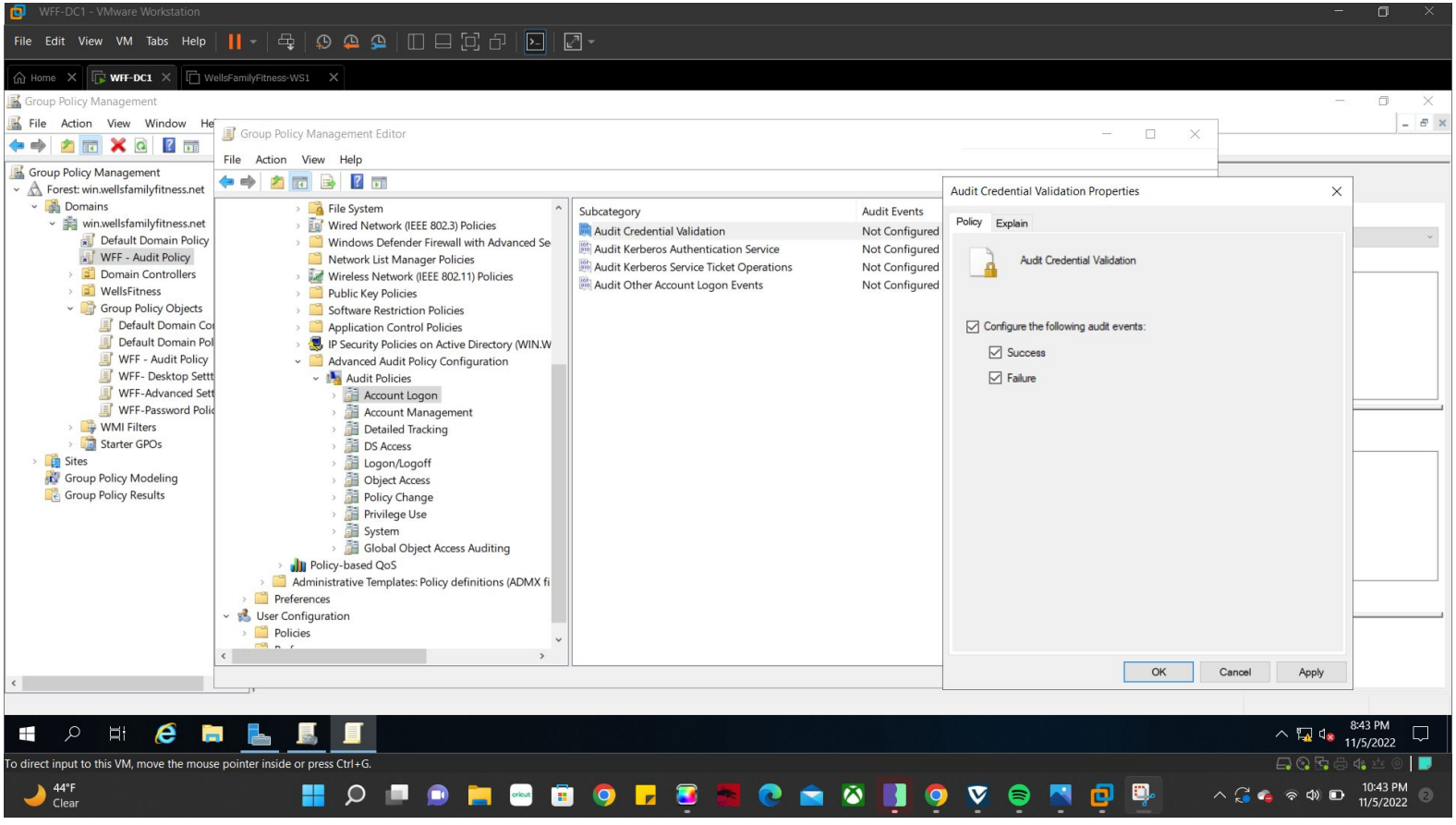



WFF-DC1 - VMware Workstation
File Edit View VM Tabs Help
Home
WFF-DC1
WellsFamilyFitness-WS1
Group Policy Management
File Action View Window He
Group Policy Management
Forest: win.wellsfamilyfitness.net
Domains
win.wellsfamilyfitness.net
Default Domain Policy
WFF - Audit Policy
Domain Controllers
WellsFitness
Group Policy Objects
Default Domain Co
Default Domain Pol
WFF - Audit Policy
WFF- Desktop Sett
WFF-Advanced Set
WFF-Password Polic
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
WFF - Audit Policy [WFF-DC1.WI
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences
WFF - Audit Policy [WFF-DC1.WIN.WELLSFAMILYFITNESS.NET] Policy
Select an item to view its description.
Name
Computer Configuration
User Configuration
Extended
Standard
<none>
Open
8:39 PM
11/5/2022
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
44°F
Clear
10:39 PM
11/5/2022

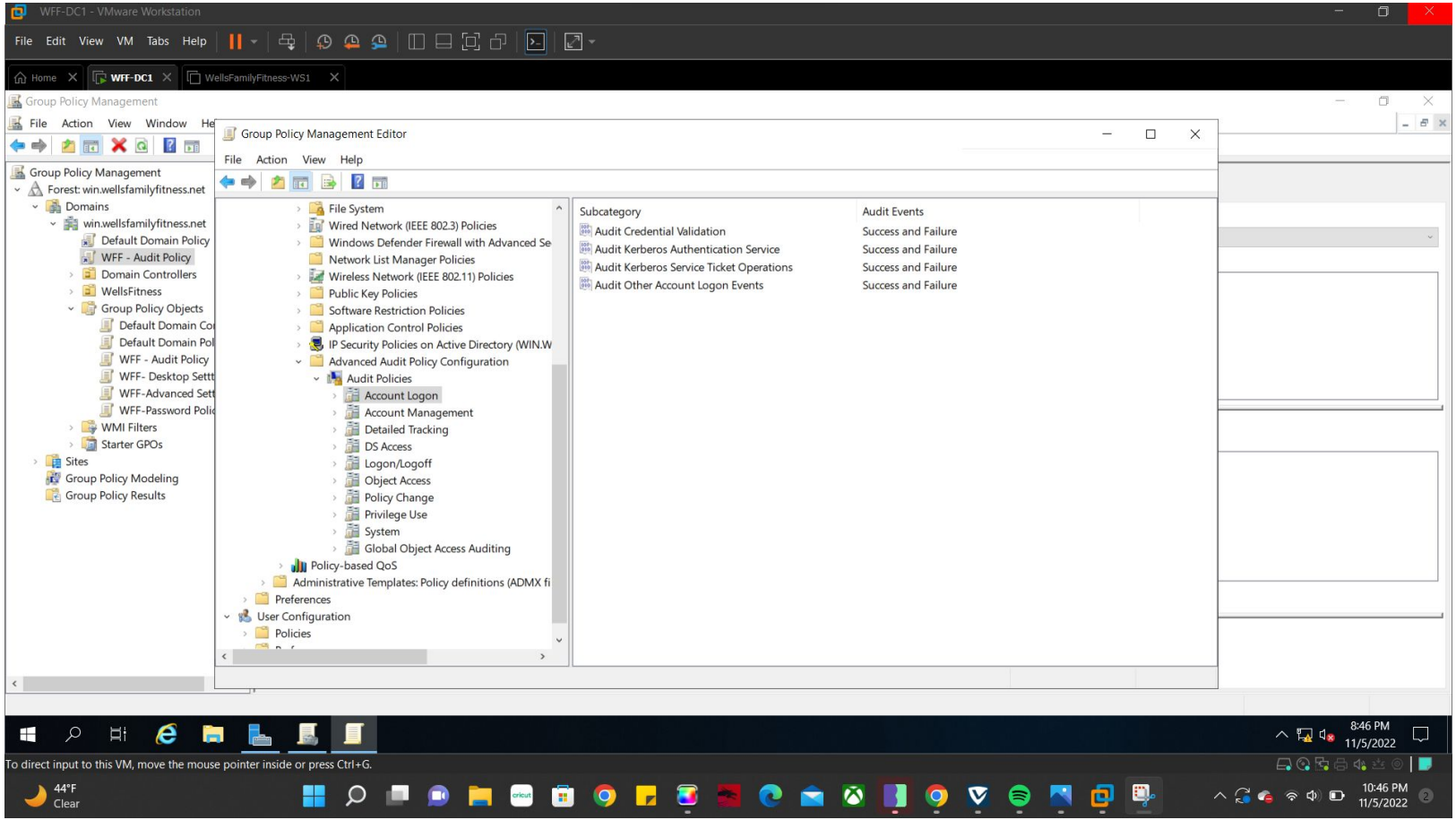
4. Then go to Windows Serttings- Advanced Audit Policy Configuration (there are also some policies located in local policies)



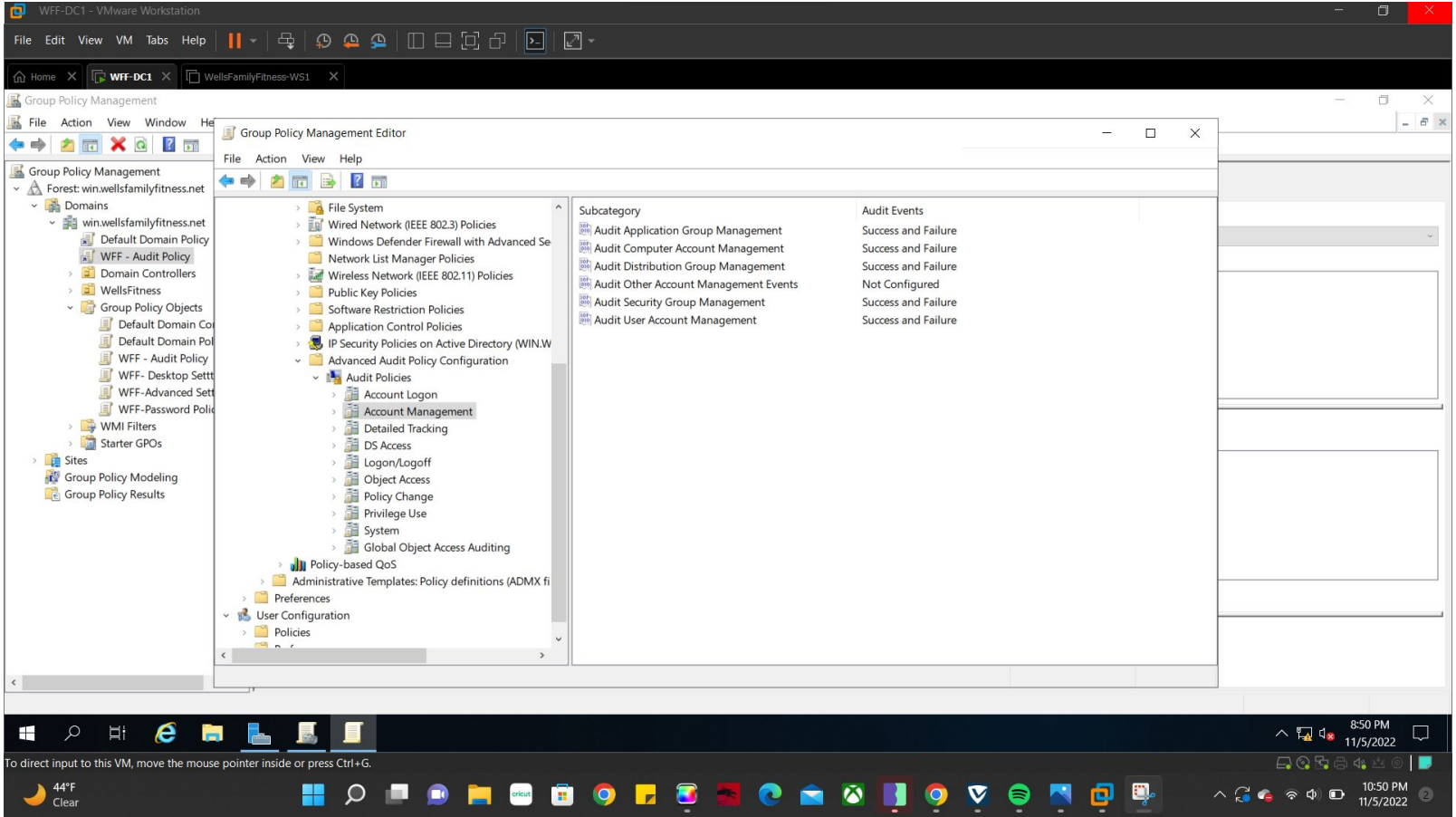
5. Each tab will has each of the audits we need to complete within in them. For account cred validation, click on Account login then Audit Credential validation. Select Configure the following… then success and failure then select ok.



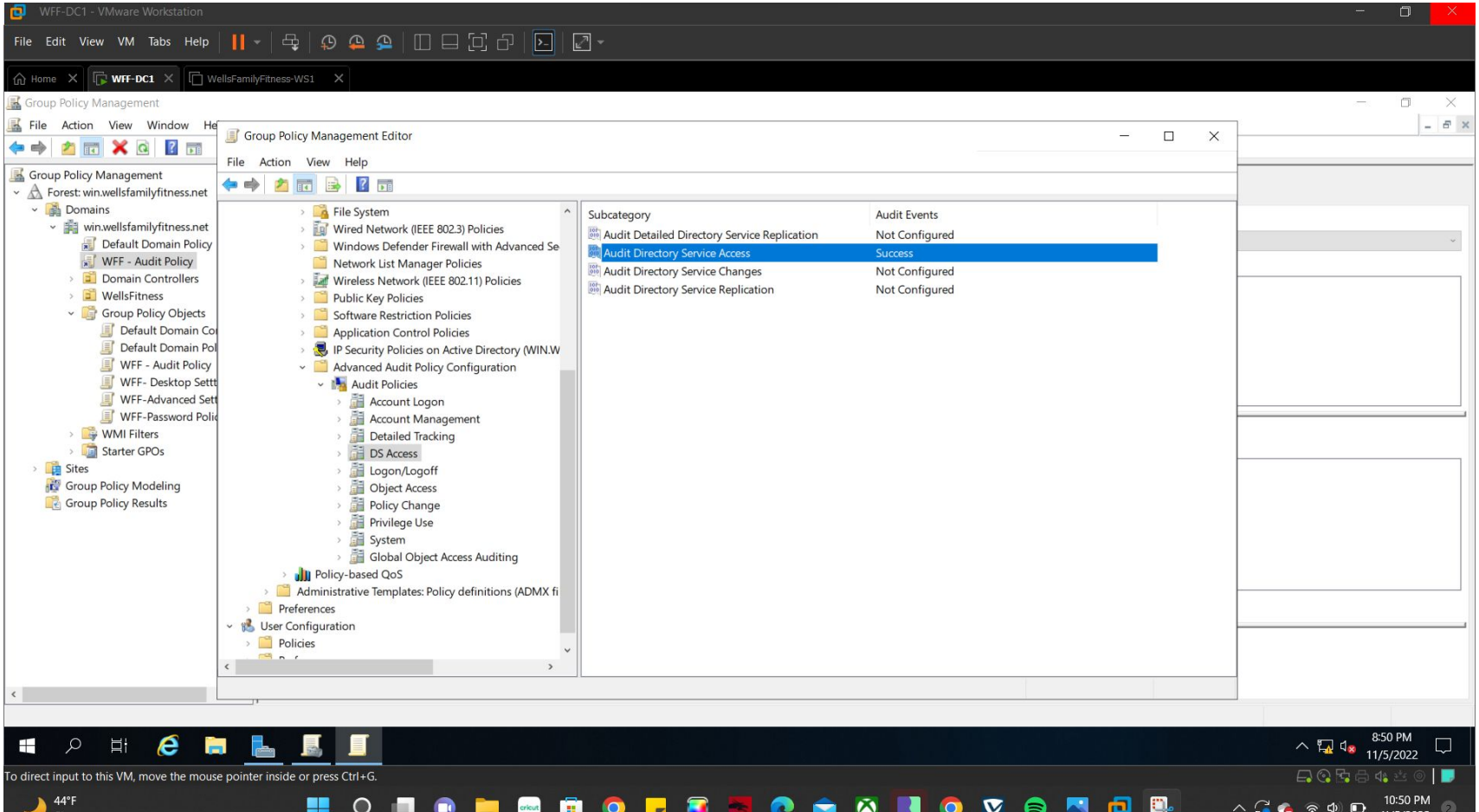
6. Repeat step five for all of the relevant settings within the Account Logon tab



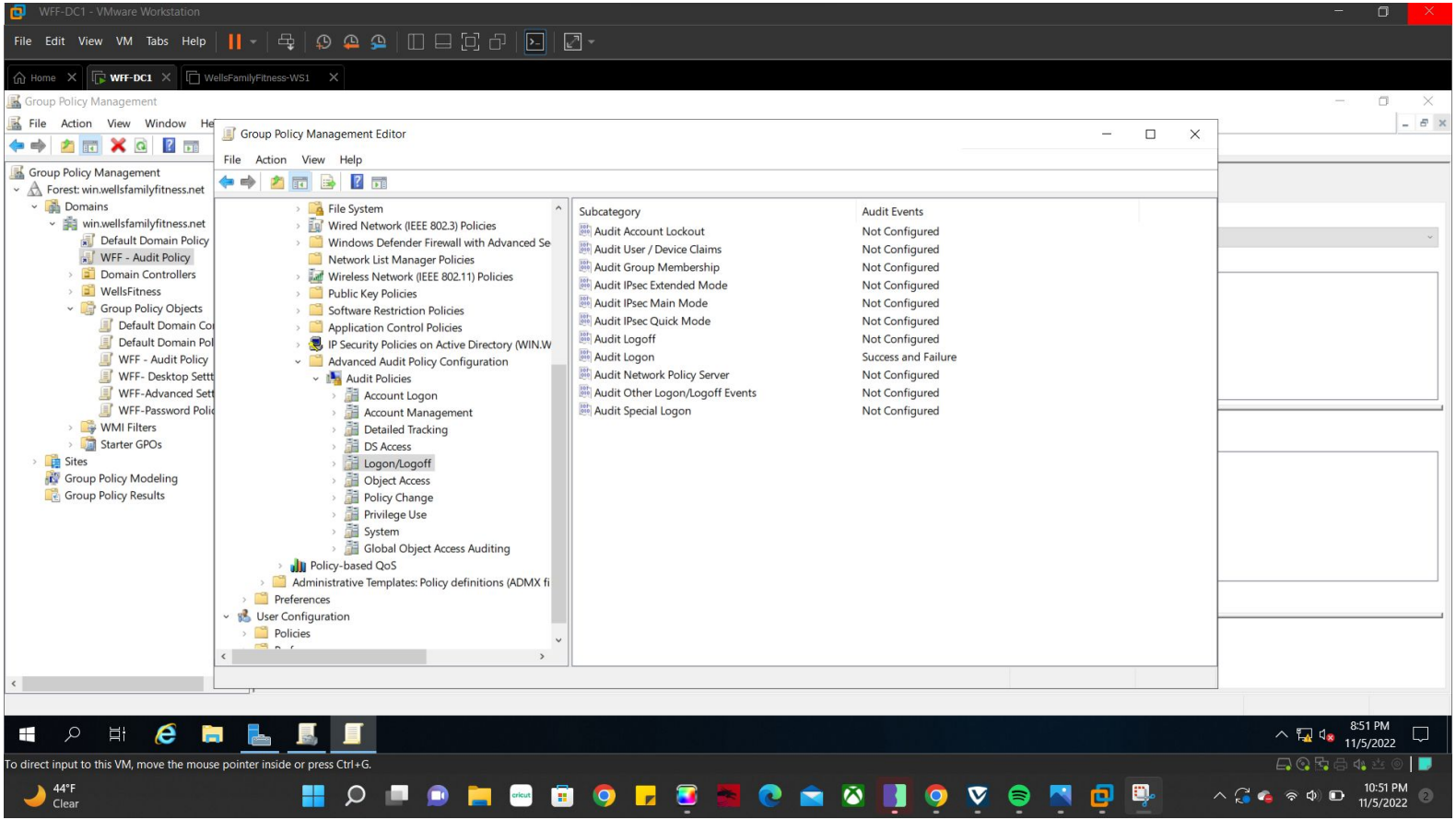
7. Account Management is next, repeat the same process as in step six for the relevant settings



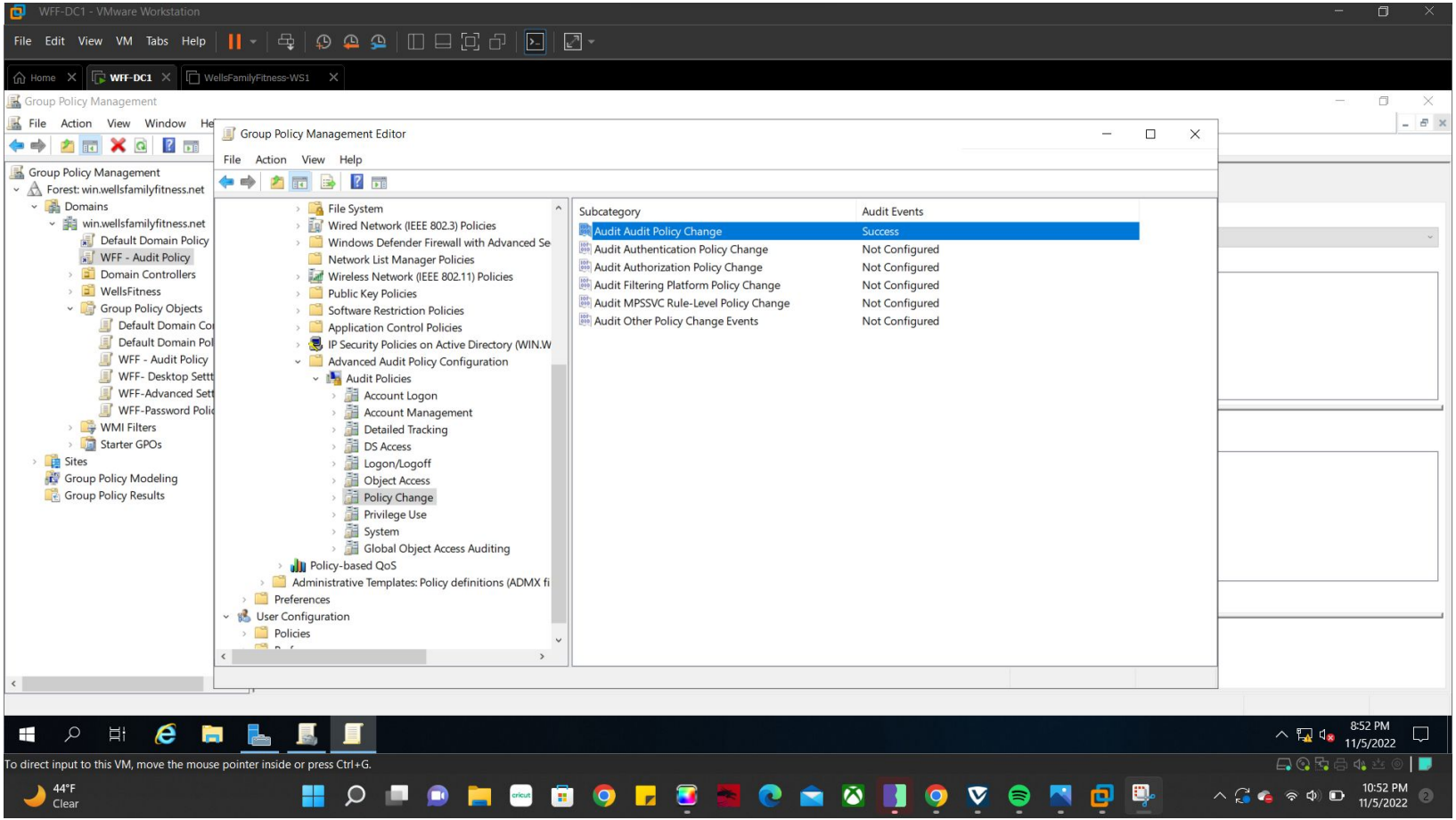
8. For DS Access, there is only one setting that needs to be edited and only select configure… and Success



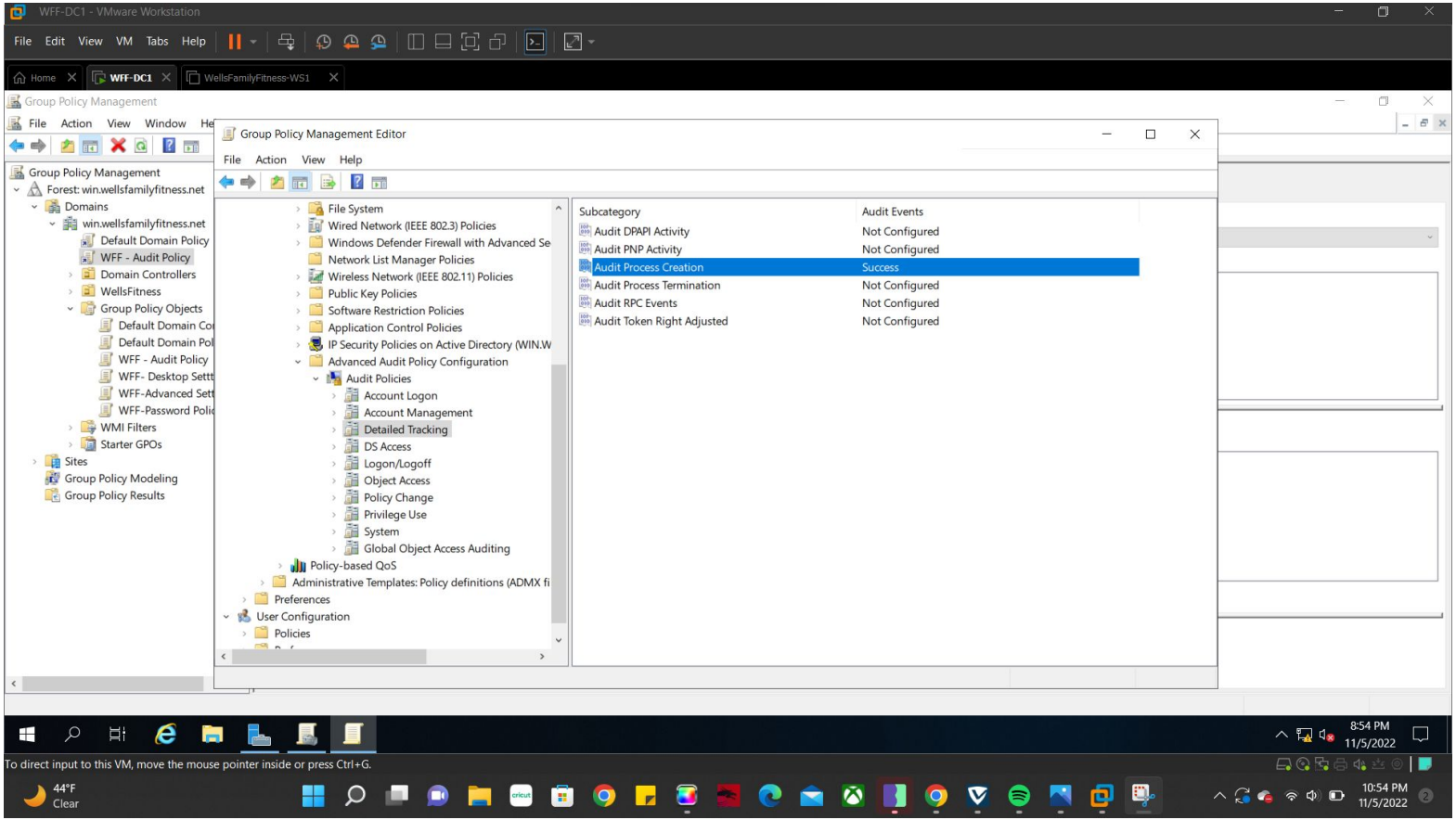
9. Repeat the same steps for audit logon



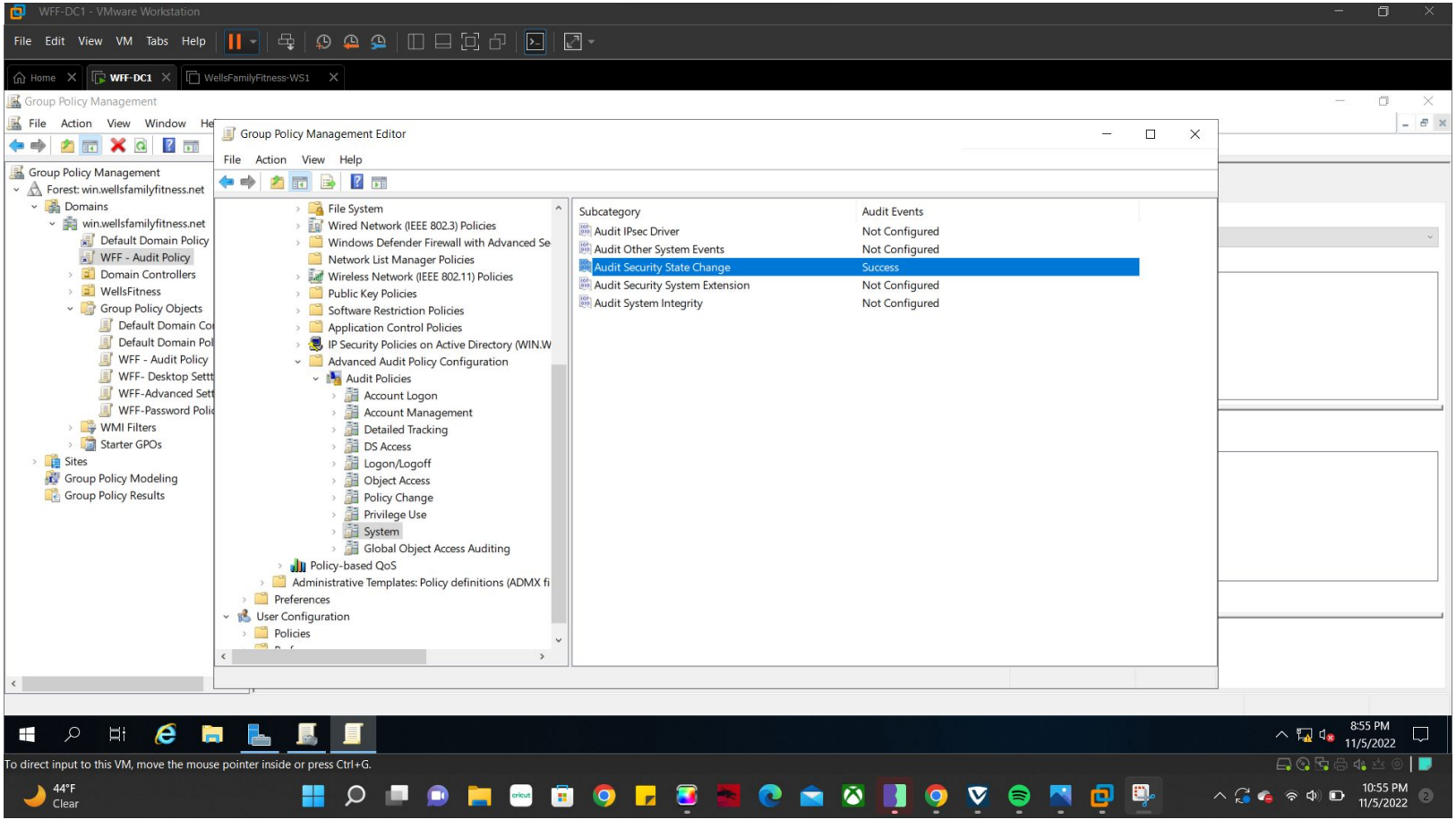
10. Same settings for Audit Audit Policy Change



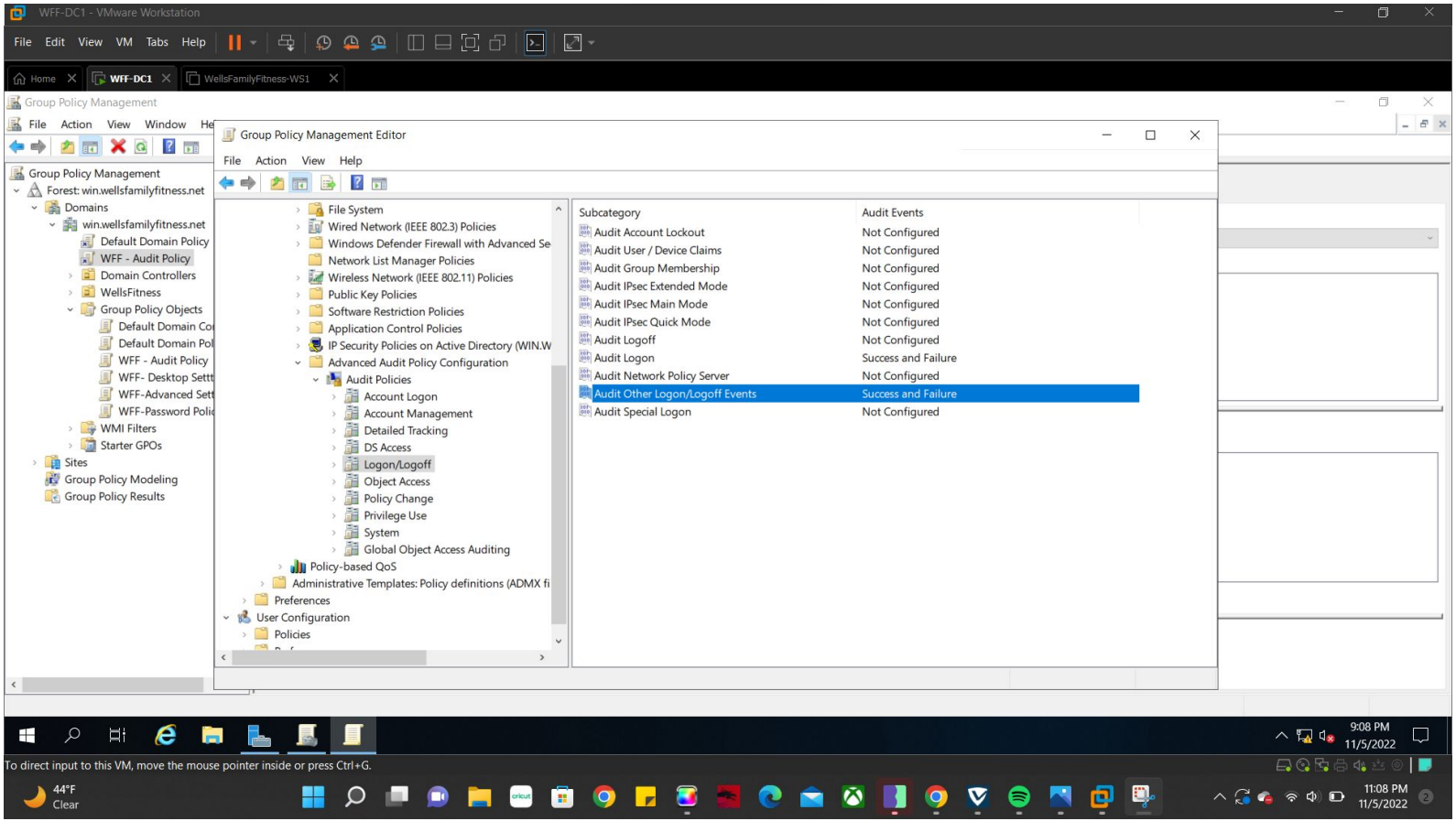
11. …and Audit Policy Creation

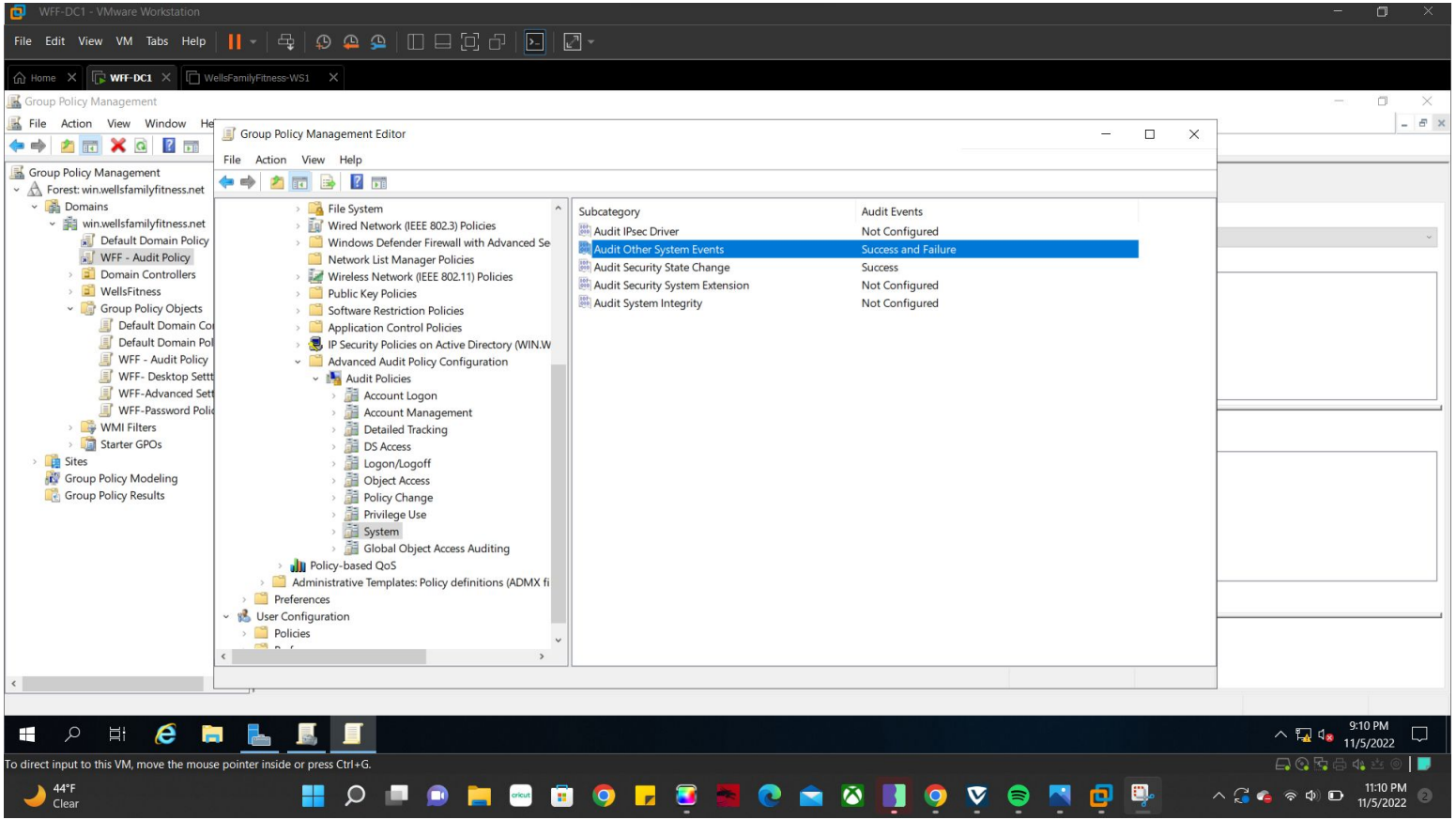


12. Under the System tab change Audit Security State Change to Success

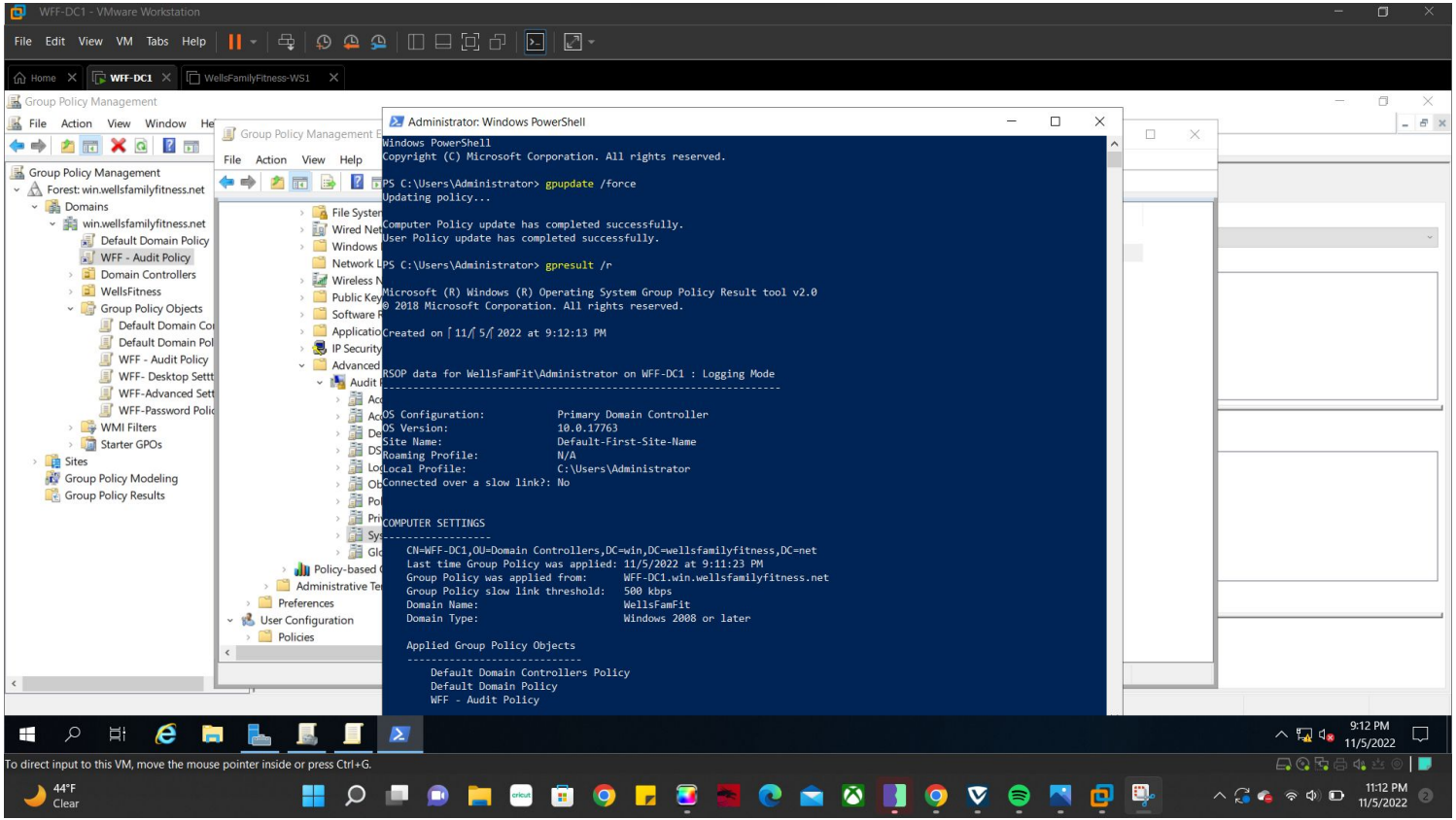


13. Change Audit Other Logon/off Events to be Success and Failure

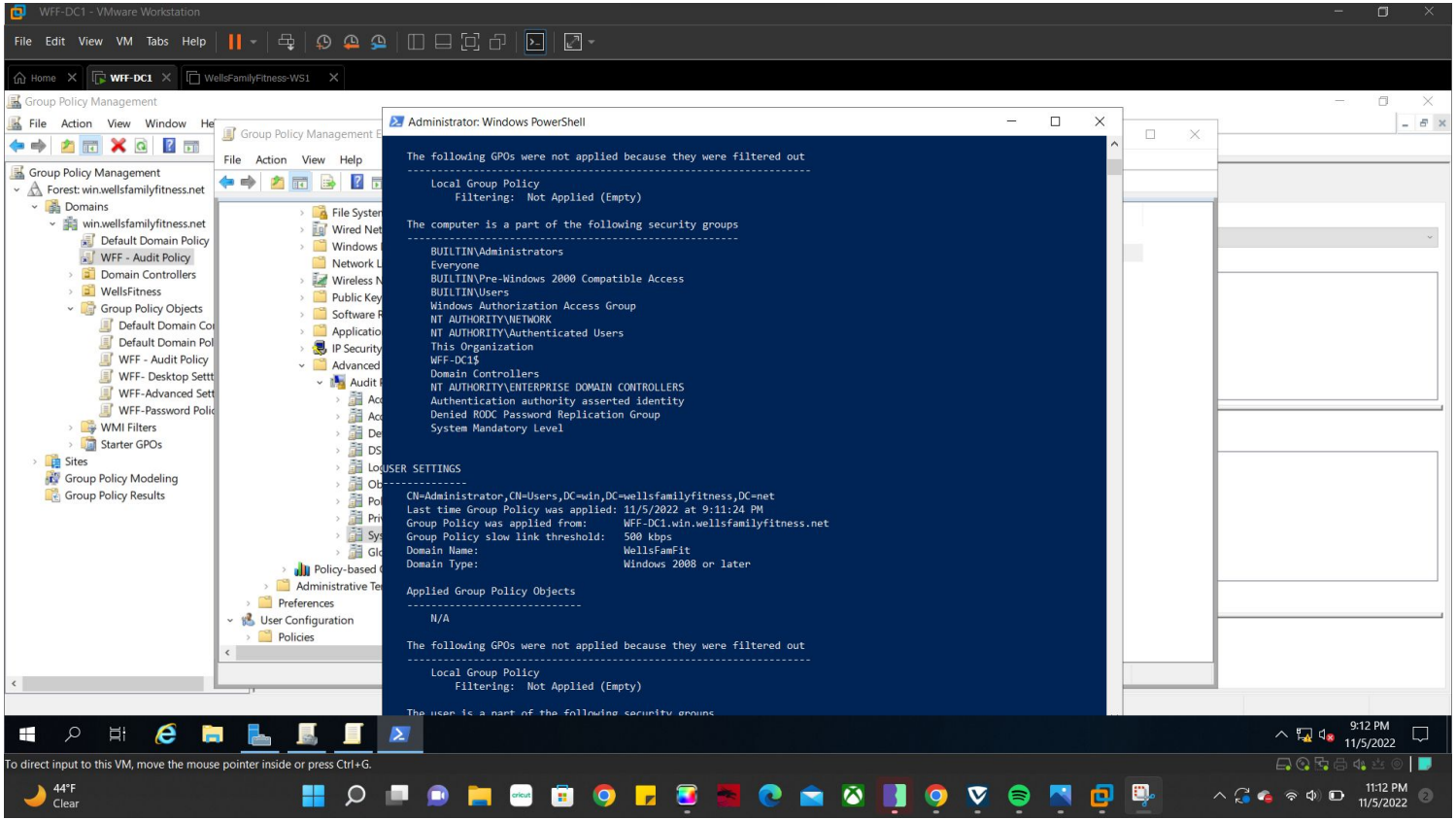



WFF-DC1 - VMware Workstation
File Edit View VM Tabs Help
Home
WFF-DC1
WellsFamilyFitness-WS1
Group Policy Management
File Action View Window
Group Policy Management
Forest: win.wellsfamilyfitness.net
Domains
win.wellsfamilyfitness.net
Default Domain Policy
WFF - Audit Policy
Domain Controllers
WellsFitness
Group Policy Objects
Default Domain Co
Default Domain Pol
WFF - Audit Policy
WFF- Desktop Sett
WFF-Advanced Sett
WFF-Password Polic
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Se
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (WIN.W
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Policy-based QoS
Administrative Templates: Policy definitions (ADMX fi
Preferences
User Configuration
Policies
Subcategory
Audit Events
Audit IPsec Driver
Not Configured
Audit Other System Events
Success and Failure
Audit Security State Change
Success
Audit Security System Extension
Not Configured
Audit System Integrity
Not Configured
9:10 PM
11/5/2022
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
44°F
Clear
11:10 PM
11/5/2022

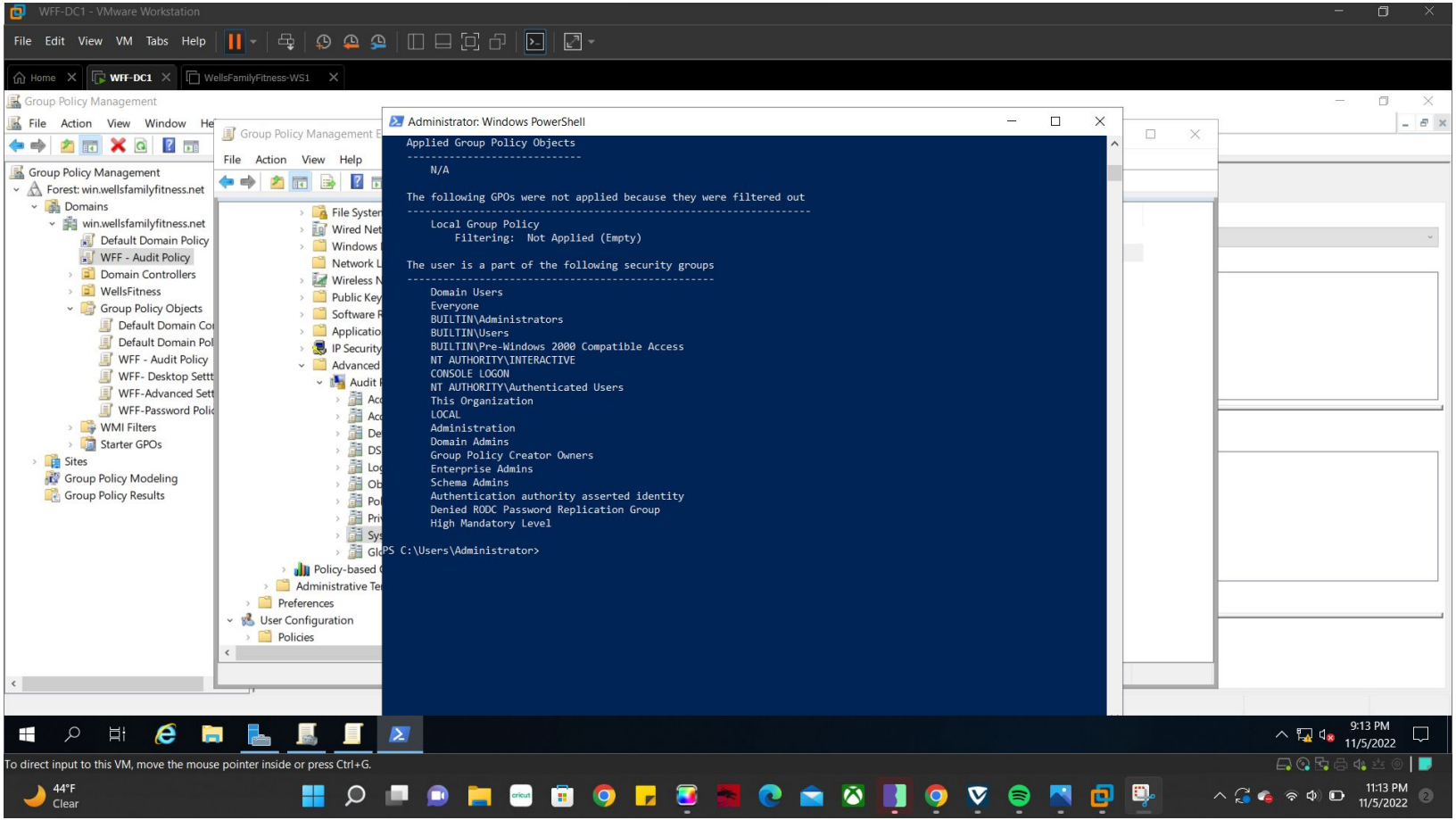
15. After making all of the audit policy changes, run powershell as administrator and type in the gpupdate /force command followed by the gpresult /r command to ensure that the policy changes did go through successfully

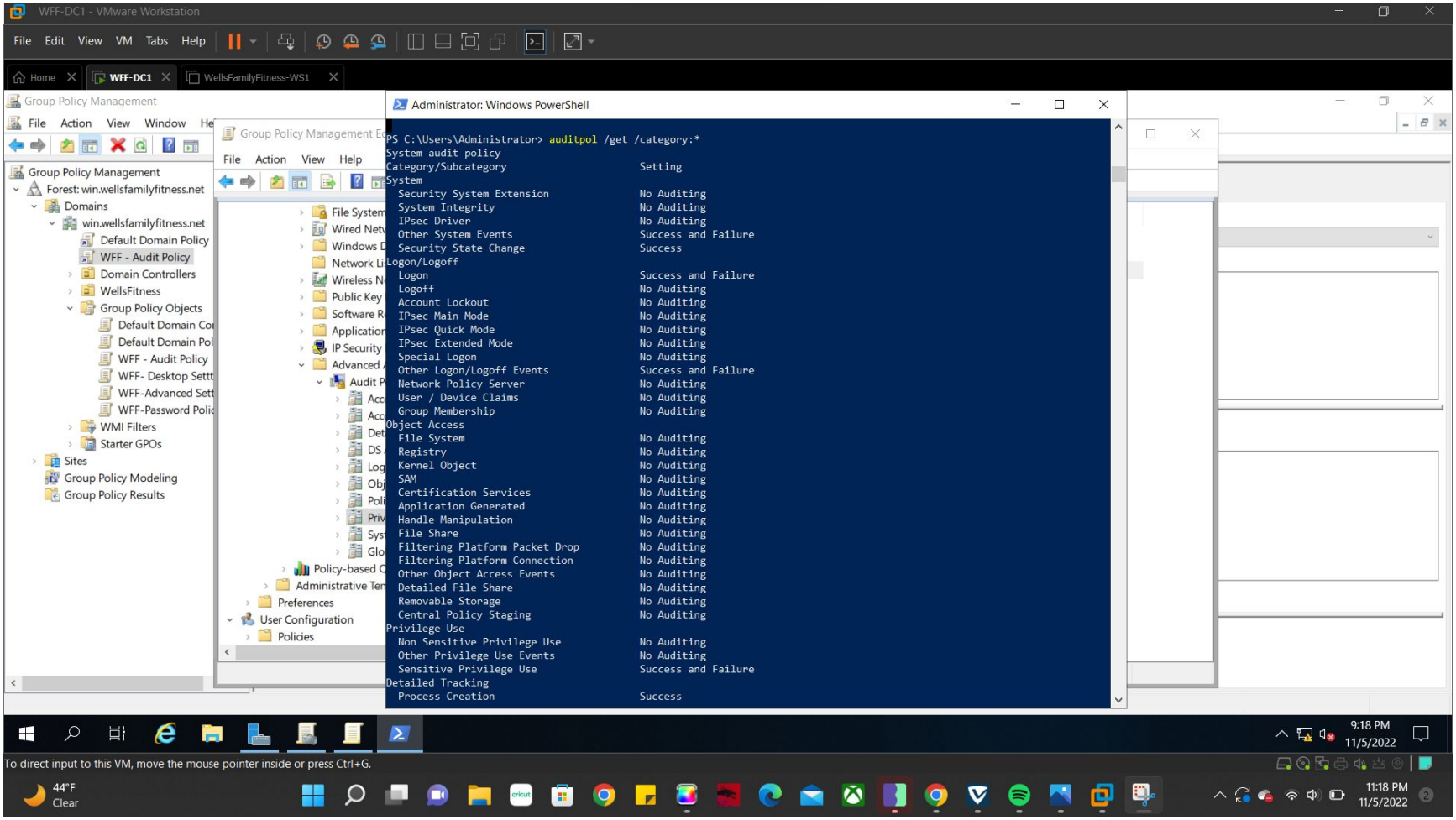


16. Step 15 continued…

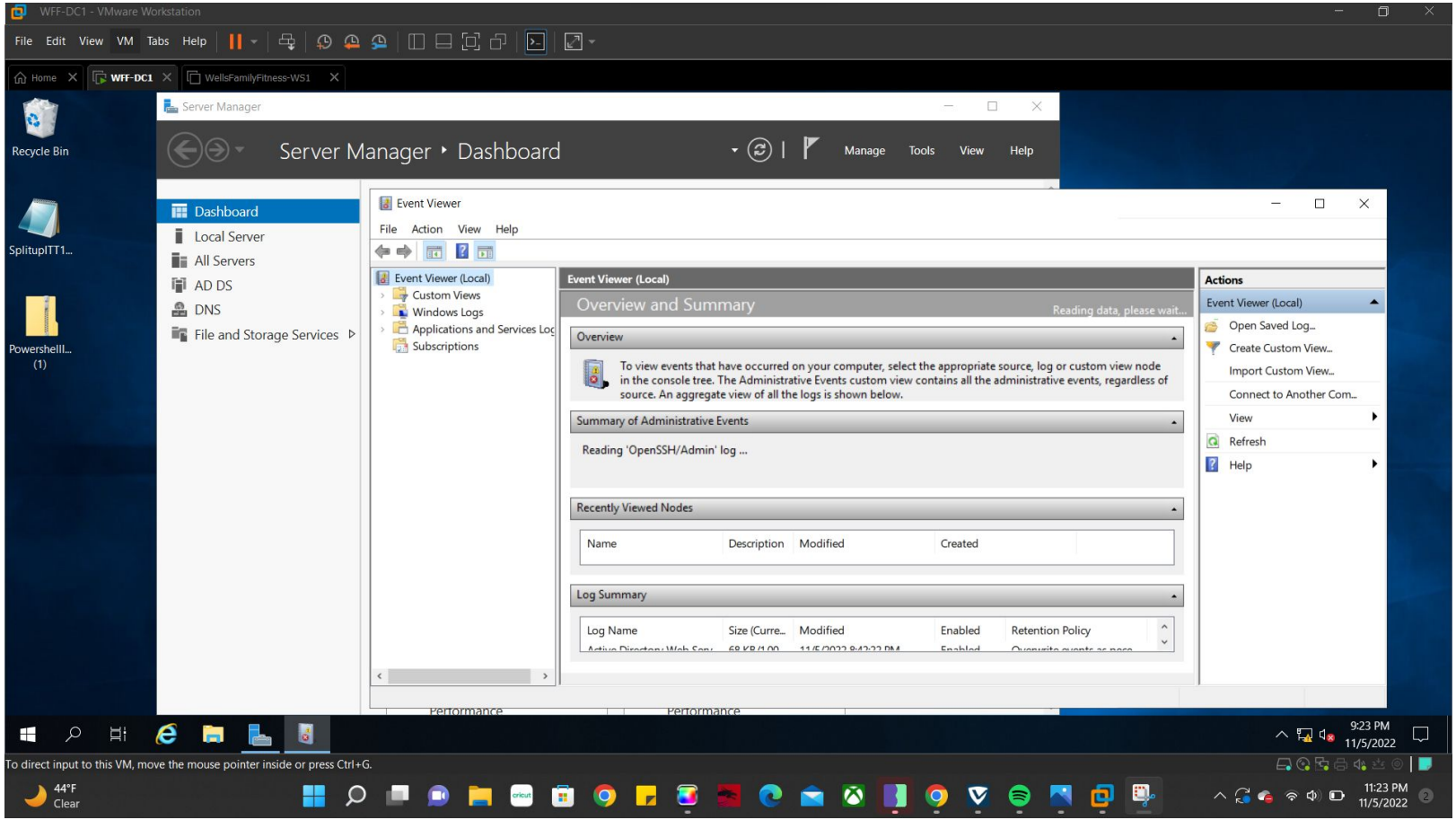


17. 15 continued

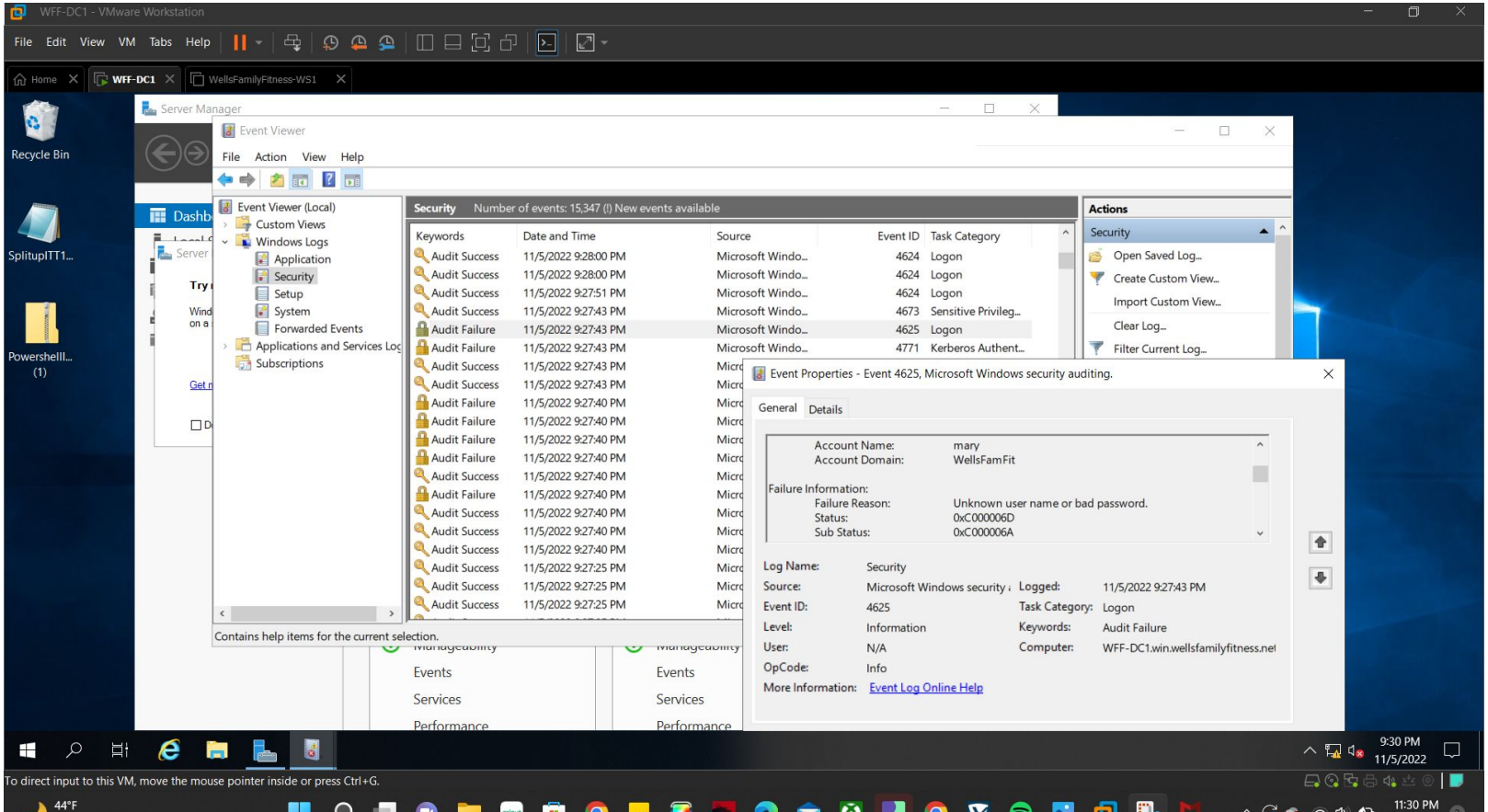



WFF-DC1 - VMware Workstation
File Edit View VM Tabs Help
Home
WFF-DC1
WellsFamilyFitness-WS1
Group Policy Management
File Action View Window
Group Policy Management
Forest: win.wellsfamilyfitness.net
Domains
win.wellsfamilyfitness.net
Default Domain Policy
WFF - Audit Policy
Domain Controllers
WellsFitness
Group Policy Objects
WFF - Audit Policy
WFF- Desktop Sett
WFF-Advanced Sett
WFF-Password Polic
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Ed
File Action View Help
Preferences
User Configuration
Policies
Administrator: Windows PowerShell
PS C:\Users\Administrator> auditpol /get /category:*
System audit policy
Category/Subcategory Setting
System
Security System Extension No Auditing
System Integrity No Auditing
IPsec Driver No Auditing
Other System Events Success and Failure
Security State Change Success
Logon/Logoff
Logon Success and Failure
Logoff No Auditing
Account Lockout No Auditing
IPsec Main Mode No Auditing
IPsec Quick Mode No Auditing
IPsec Extended Mode No Auditing
Special Logon No Auditing
Other Logon/Logoff Events Success and Failure
Network Policy Server No Auditing
User / Device Claims No Auditing
Group Membership No Auditing
Object Access
File System No Auditing
Registry No Auditing
Kernel Object No Auditing
SAM No Auditing
Certification Services No Auditing
Application Generated No Auditing
Handle Manipulation No Auditing
File Share No Auditing
Filtering Platform Packet Drop No Auditing
Filtering Platform Connection No Auditing
Other Object Access Events No Auditing
Detailed File Share No Auditing
Removable Storage No Auditing
Central Policy Staging No Auditing
Privilege Use
Non Sensitive Privilege Use No Auditing
Other Privilege Use Events No Auditing
Sensitive Privilege Use Success and Failure
Detailed Tracking
Process Creation Success
9:18 PM
11/5/2022
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
44°F
Clear
11:18 PM
11/5/2022

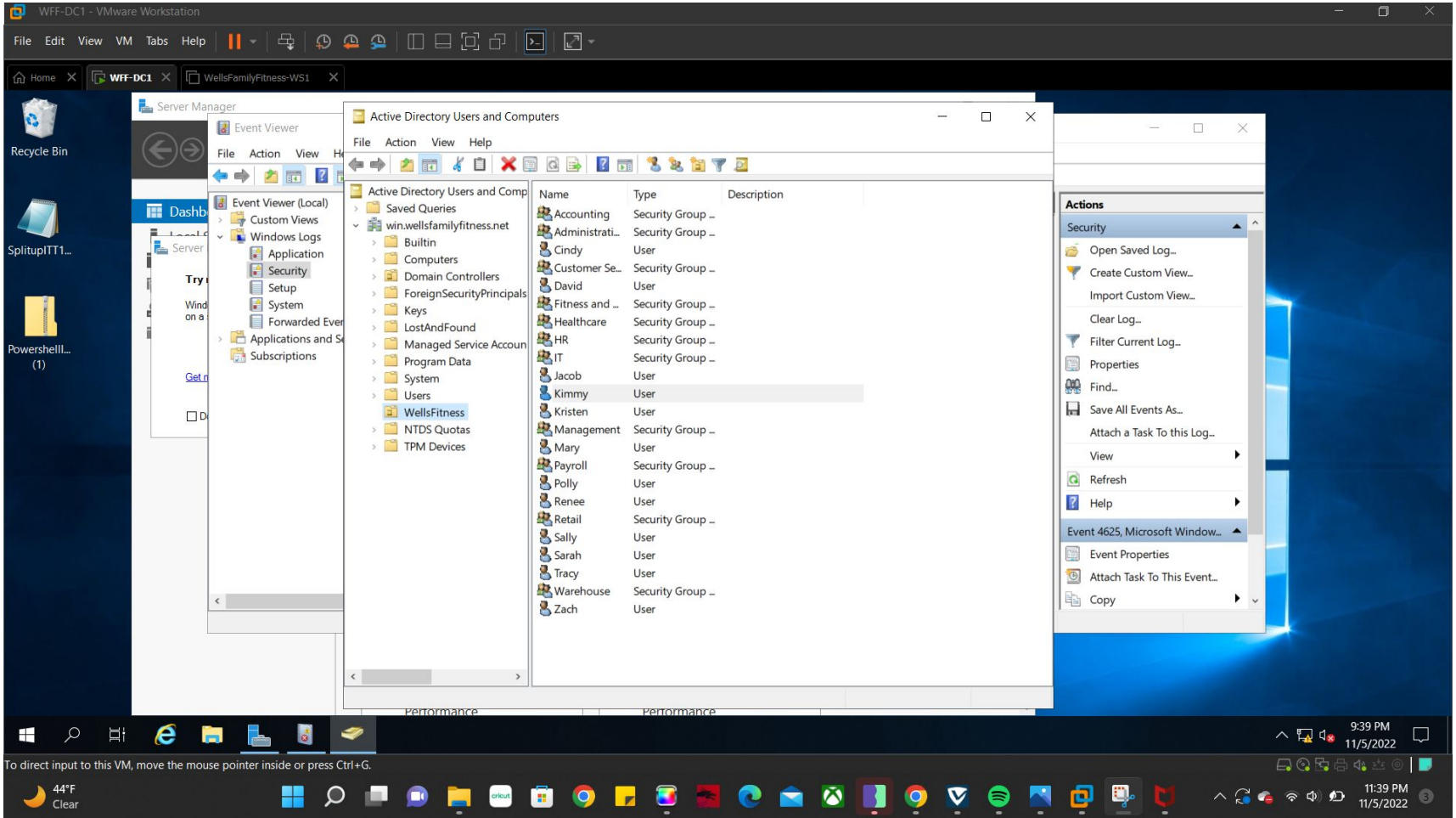
19. After testing a failed log on as an additional user log back into your admin account and open event viewer



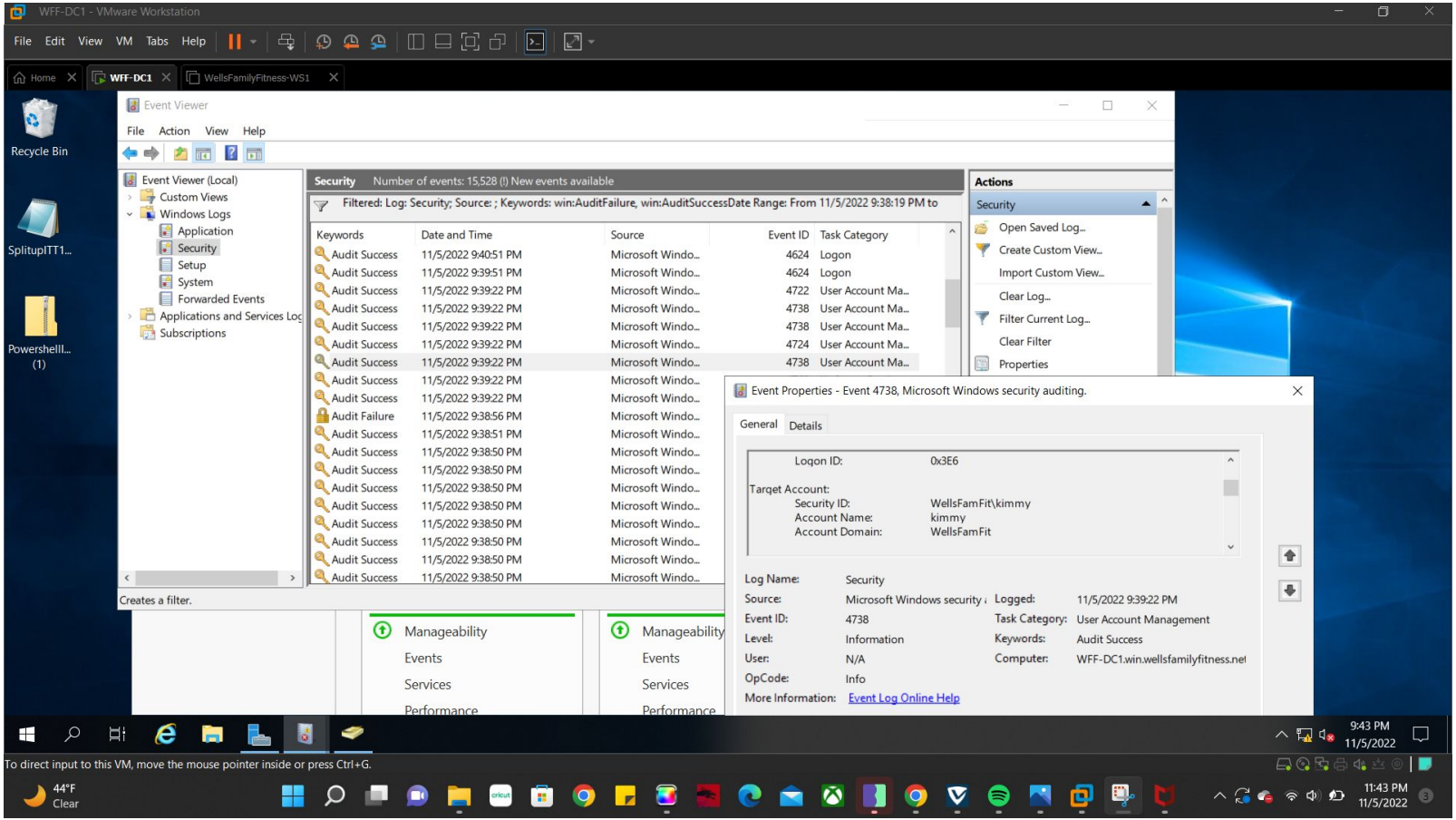
20. You should be able to find the audit failure event and its details of the failed logon attempt



21. Go to Active Directory and Computers and create a new user that you will remember



22. Then go back to the event viewer and you will also be able to find the audit success event /details of when and the account you just created



23. Log on to the workstation, once purposely entering the wrong password and then successfully. As a user (with administrator login) you can run the event viewer on a workstation and see the audit failure event of the logon failed attempt.