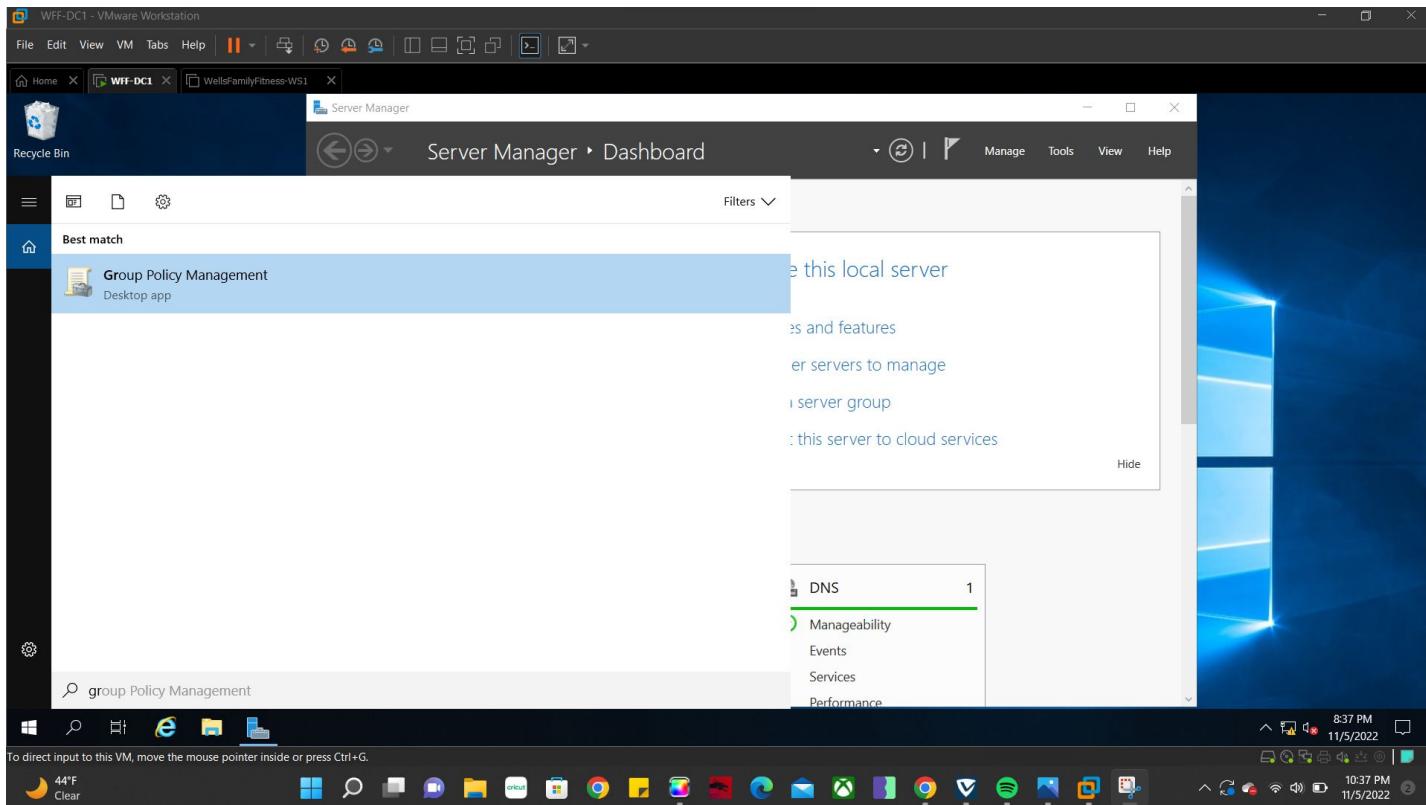


1. In the DC server open Group Policy Management as Administrator

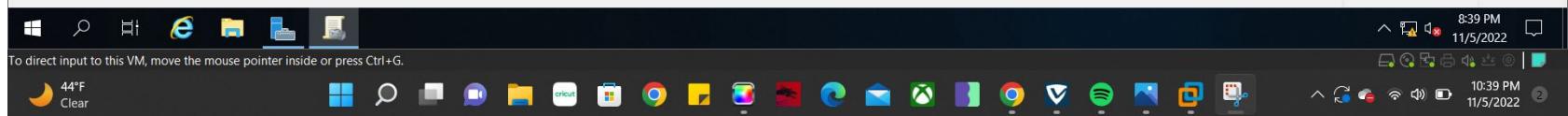
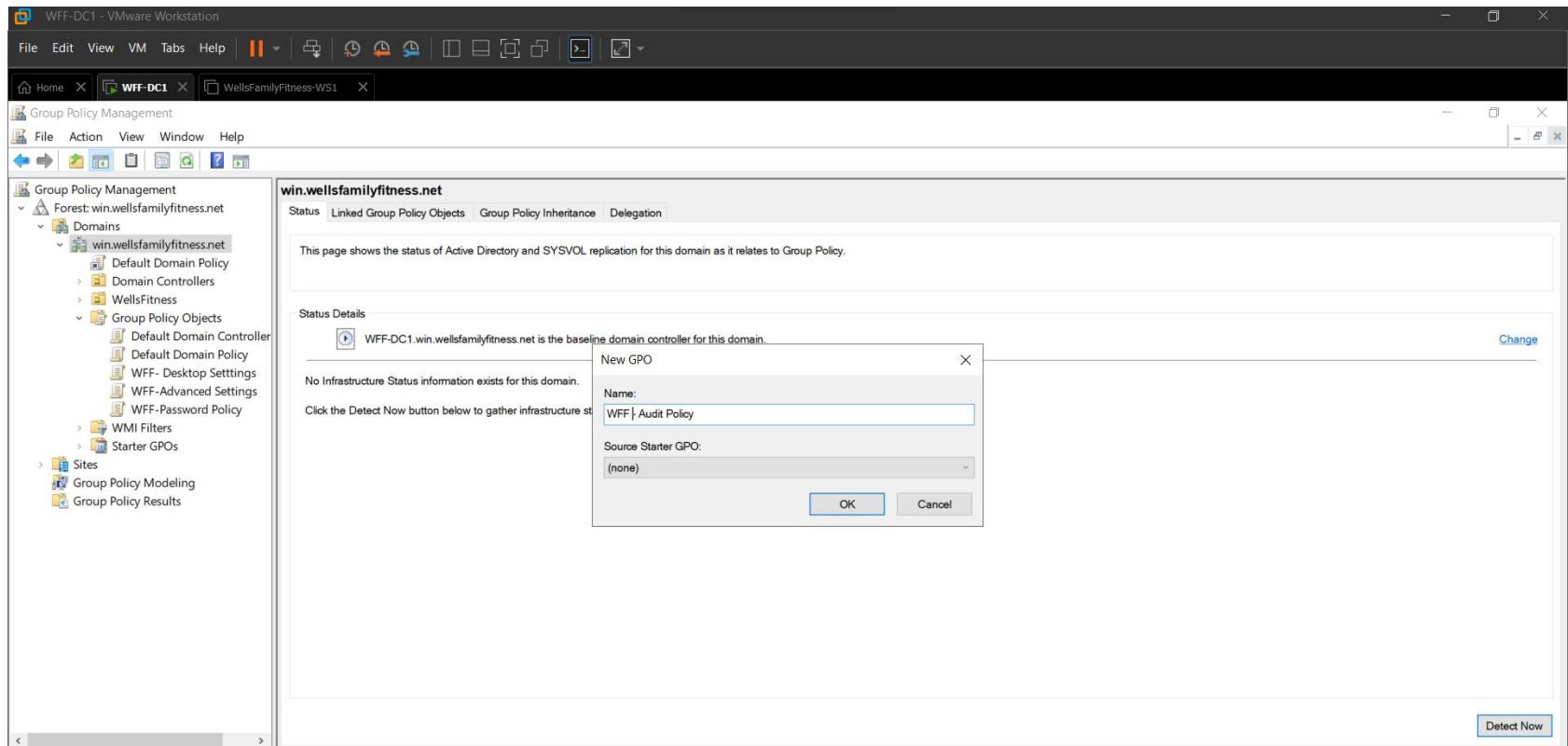


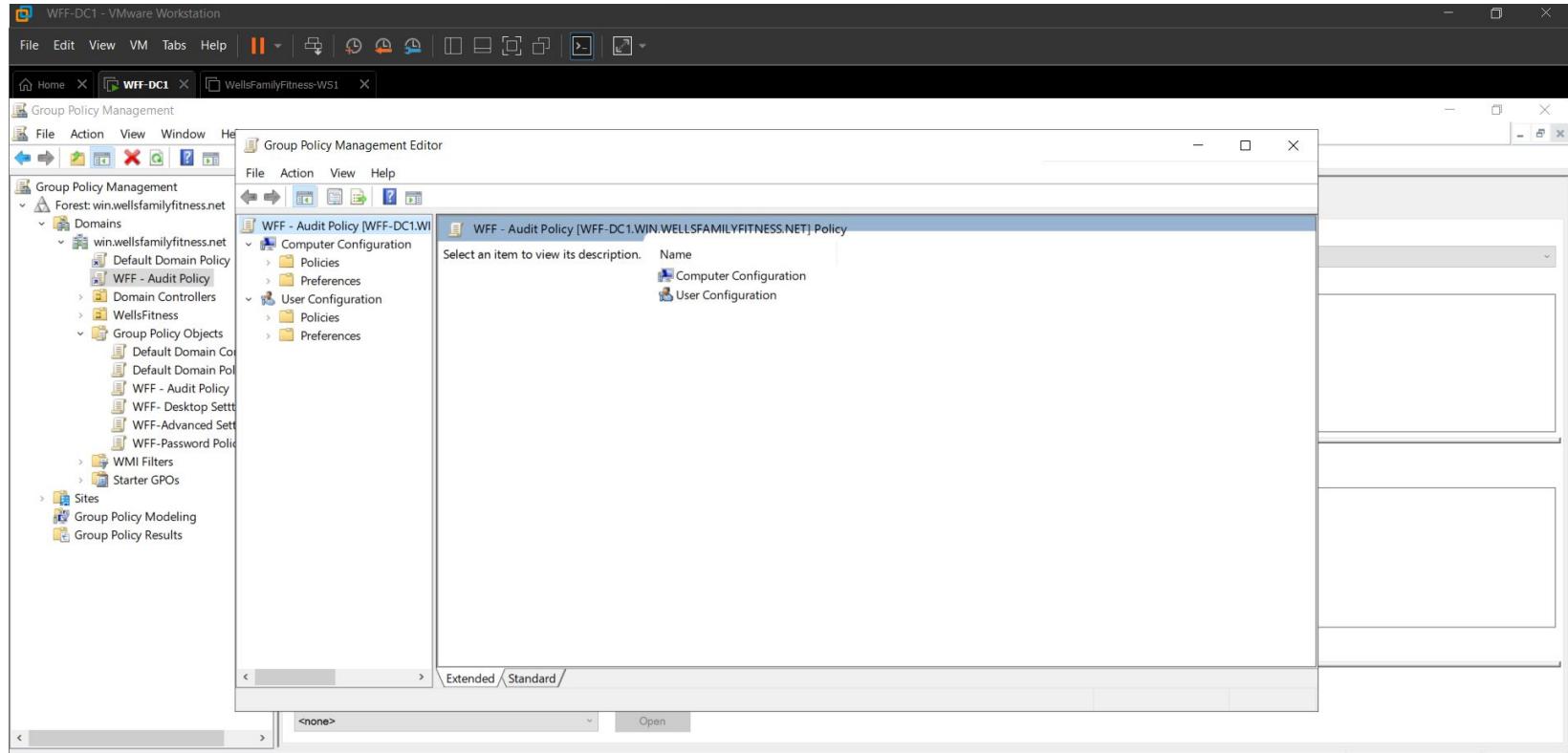
# AUDITING COMMON THREATS ON VMWARE-WINDOWS SERVER 2016

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





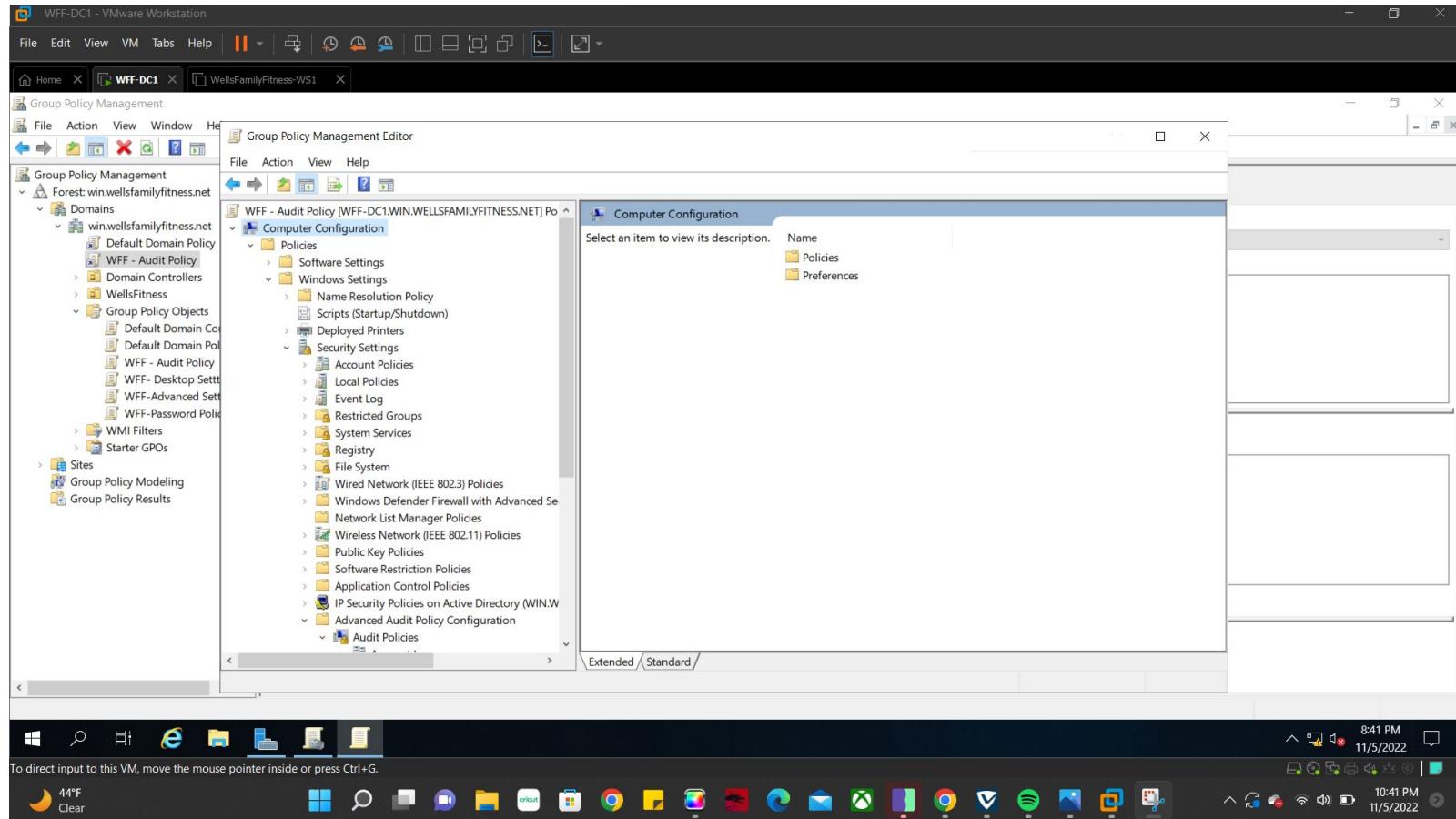
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

44°F  
Clear

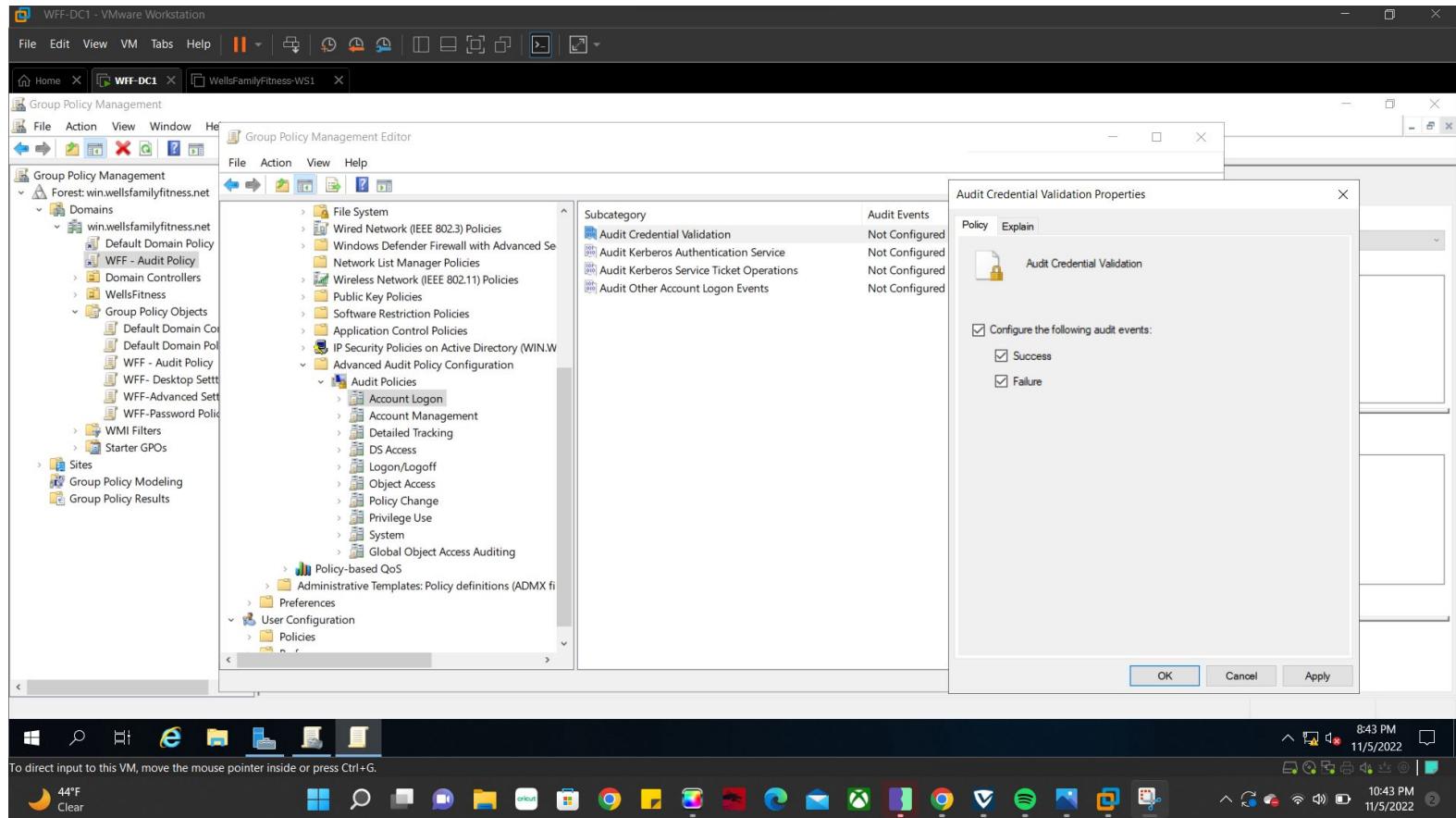


8:39 PM  
11/5/2022  
File  
Print  
Share  
Help  
10:39 PM  
11/5/2022

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



5. Each tab will have each of the audits we need to complete within 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

The screenshot shows the Windows Group Policy Management Editor window titled "Group Policy Management Editor". The left pane displays the Group Policy Object (GPO) structure under "Forest: win.wellsfamilyfitness.net". The "WFF - Audit Policy" GPO is selected. The right pane shows the "Audit Policies" section under "File System". A table lists audit categories and their sub-categories and success/failure events:

Subcategory	Audit Events
Audit Credential Validation	Success and Failure
Audit Kerberos Authentication Service	Success and Failure
Audit Kerberos Service Ticket Operations	Success and Failure
Audit Other Account Logon Events	Success and Failure

The taskbar at the bottom shows various pinned icons and the system tray indicates the date and time as 11/5/2022 at 8:46 PM.

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

The screenshot shows a Windows desktop environment with a VMware Workstation window titled "WFF-DC1 - VMware Workstation". Inside the window, the "Group Policy Management Editor" is open. The left pane displays a tree view of Group Policy Objects (GPOs) under "Forest: win.wellsfamilyfitness.net". One GPO, "WFF - Audit Policy", is selected. The right pane shows the "Audit Policies" section of the editor. A table lists various audit policies and their subcategories and audit events:

Subcategory	Audit Events
Audit Application Group Management	Success and Failure
Audit Computer Account Management	Success and Failure
Audit Distribution Group Management	Success and Failure
Audit Other Account Management Events	Not Configured
Audit Security Group Management	Success and Failure
Audit User Account Management	Success and Failure
Account Logon	
Account Management	
Detailed Tracking	
DS Access	
Logon/Logoff	
Object Access	
Policy Change	
Privilege Use	
System	
Global Object Access Auditing	

The status bar at the bottom of the screen shows the date and time as "11/5/2022 8:50 PM".

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

The screenshot shows the Windows Group Policy Management Editor running in a VMware Workstation window. The left pane displays the Group Policy Management structure for the 'win.wellsfamilyfitness.net' forest. The 'Audit Policies' section under 'Advanced Audit Policy Configuration' is selected. In the center pane, the 'Audit Directory Service Access' policy is highlighted, showing its status as 'Success'. The right pane is currently empty.

Group Policy Management Editor

File Action View Help

Subcategory

Subcategory	Audit Events	Status
Audit Detailed Directory Service Replication	Not Configured	
<b>Audit Directory Service Access</b>	<b>Success</b>	
Audit Directory Service Changes	Not Configured	
Audit Directory Service Replication	Not Configured	

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

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

8:50 PM 11/5/2022

44°F

10:50 PM

## 9. Repeat the same steps for audit logon

The screenshot shows the Windows Group Policy Management Editor window titled "Group Policy Management Editor". The left pane displays the Group Policy Management structure for the "win.wellsfamilyfitness.net" forest, specifically under the "WFF - Audit Policy" GPO. The right pane shows the "Audit Policies" section of the "Advanced Audit Policy Configuration" node. A table lists various audit events and their current status:

Subcategory	Audit Events
Audit Account Lockout	Not Configured
Audit User / Device Claims	Not Configured
Audit Group Membership	Not Configured
Audit IPsec Extended Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit Logoff	Not Configured
Audit Logon	Success and Failure
Audit Network Policy Server	Not Configured
Audit Other Logon/Logoff Events	Not Configured
Audit Special Logon	Not Configured

The status column indicates that most audit events are currently "Not Configured". The "Audit Logon" event is set to "Success and Failure".

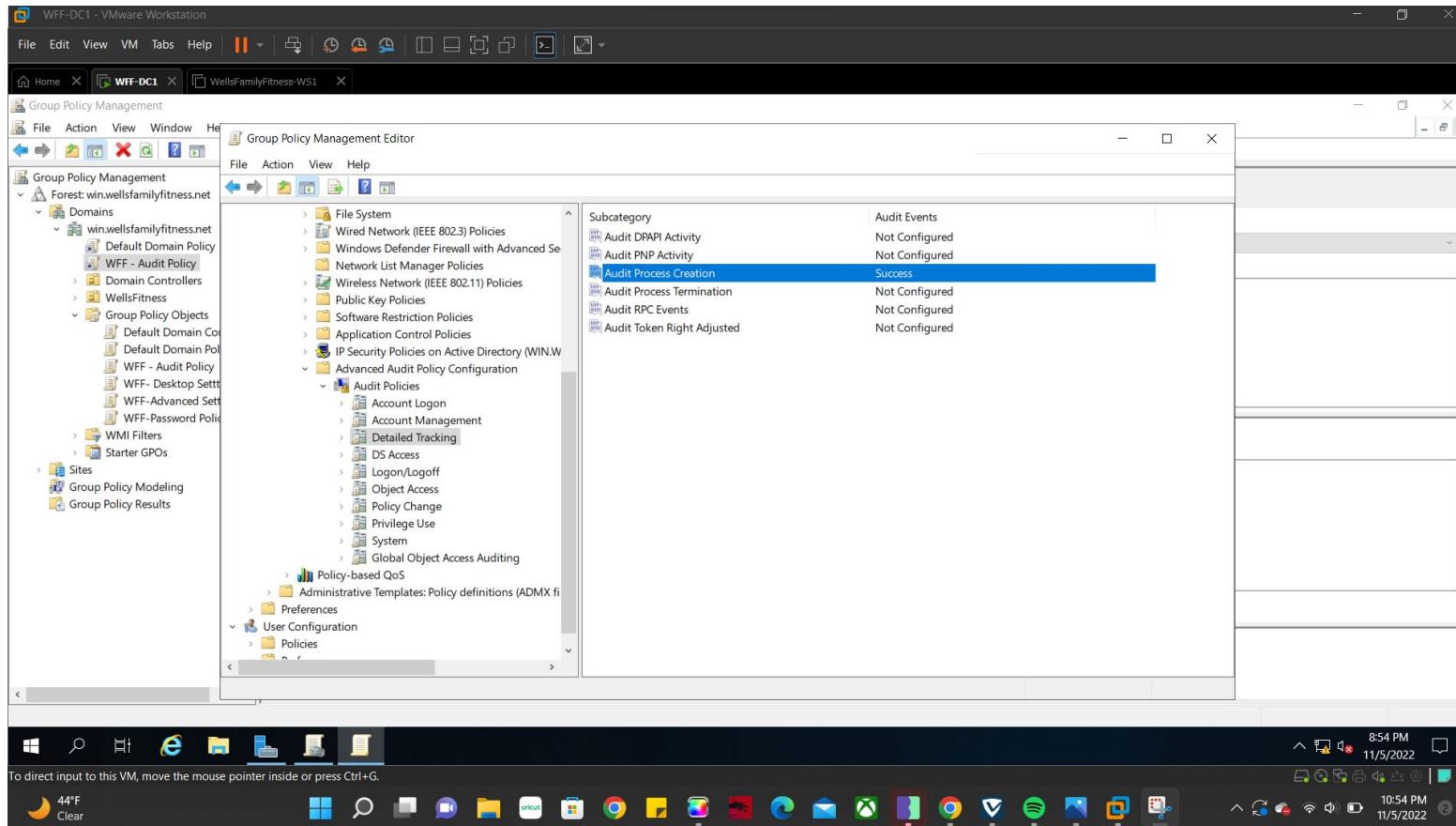
## 10. Same settings for Audit Audit Policy Change

The screenshot shows the Windows Group Policy Management Editor window titled "WFF-DC1 - VMware Workstation". The left pane displays the Group Policy Management tree for the forest "win.wellsfamilyfitness.net". The "Audit Policies" node under "Advanced Audit Policy Configuration" is selected. The right pane shows the "Audit Events" table for the "Audit Audit Policy Change" subcategory.

Subcategory	Audit Events
Audit Audit Policy Change	Success
Audit Authentication Policy Change	Not Configured
Audit Authorization Policy Change	Not Configured
Audit Filtering Platform Policy Change	Not Configured
Audit MPSSVC Rule-Level Policy Change	Not Configured
Audit Other Policy Change Events	Not Configured

The status bar at the bottom indicates: "To direct input to this VM, move the mouse pointer inside or press Ctrl+G." The taskbar shows various application icons, and the system tray shows the date and time as "11/5/2022 10:52 PM".

## 11. ...and Audit Policy Creation



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

The screenshot shows the Windows Group Policy Management Editor window titled "WFF-DC1 - VMware Workstation". The left pane displays the Group Policy Management structure for the "win.wellsfamilyfitness.net" forest. The "WFF - Audit Policy" node under "Default Domain Policy" is selected. The right pane shows the "Audit Events" section of the "Audit Security State Change" policy. The table lists the following configurations:

Subcategory	Audit Events
Audit IPsec Driver	Not Configured
Audit Other System Events	Not Configured
<b>Audit Security State Change</b>	<b>Success</b>
Audit Security System Extension	Not Configured
Audit System Integrity	Not Configured

The "Audit Security State Change" row is highlighted with a blue selection bar. The Windows taskbar at the bottom shows various pinned icons and the system tray with the date and time.

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

The screenshot shows a Windows desktop environment with a VMware Workstation window titled "WFF-DC1 - VMware Workstation". The main focus is the "Group Policy Management Editor" window, which is open to the "Audit Policies" section under "Advanced Audit Policy Configuration".

The left pane of the GPM Editor shows the Group Policy structure:

- Forest: win.wellsfamilyfitness.net
- Domains:
  - win.wellsfamilyfitness.net
    - Default Domain Policy
    - WFF - Audit Policy
  - Domain Controllers
  - WellsFitness
  - Group Policy Objects
    - Default Domain Configuration
    - Default Domain Policy
    - WFF - Audit Policy
    - WFF - Desktop Settings
    - WFF - Advanced Settings
    - WFF - Password Policy
  - WMI Filters
  - Starter GPOs
- Sites
- Group Policy Modeling
- Group Policy Results

The right pane displays the "Audit Policies" table:

Subcategory	Audit Events
Audit Account Lockout	Not Configured
Audit User / Device Claims	Not Configured
Audit Group Membership	Not Configured
Audit IPsec Extended Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit Logoff	Not Configured
Audit Logon	Success and Failure
Audit Network Policy Server	Not Configured
<b>Audit Other Logon/Logoff Events</b>	<b>Success and Failure</b>
Audit Special Logon	Not Configured

The "Audit Other Logon/Logoff Events" row is highlighted with a blue selection bar.

The taskbar at the bottom of the screen shows various pinned icons and the system tray with the date and time (11/5/2022) and battery level (908 PM).

WFF-DC1 - VMware Workstation

File Edit View VM Tabs Help

Home WFF-DC1 WellsFamilyFitness-WS1

Group Policy Management

File Action View Window Help

Group Policy Management Editor

File Action View Help

Subcategory

Subcategory	Audit Events
Audit IPsec Driver	Not Configured
<b>Audit Other System Events</b>	<b>Success and Failure</b>
Audit Security State Change	Success
Audit Security System Extension	Not Configured
Audit System Integrity	Not Configured

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 f  
Preferences  
User Configuration  
Policies

9:10 PM 11/5/2022

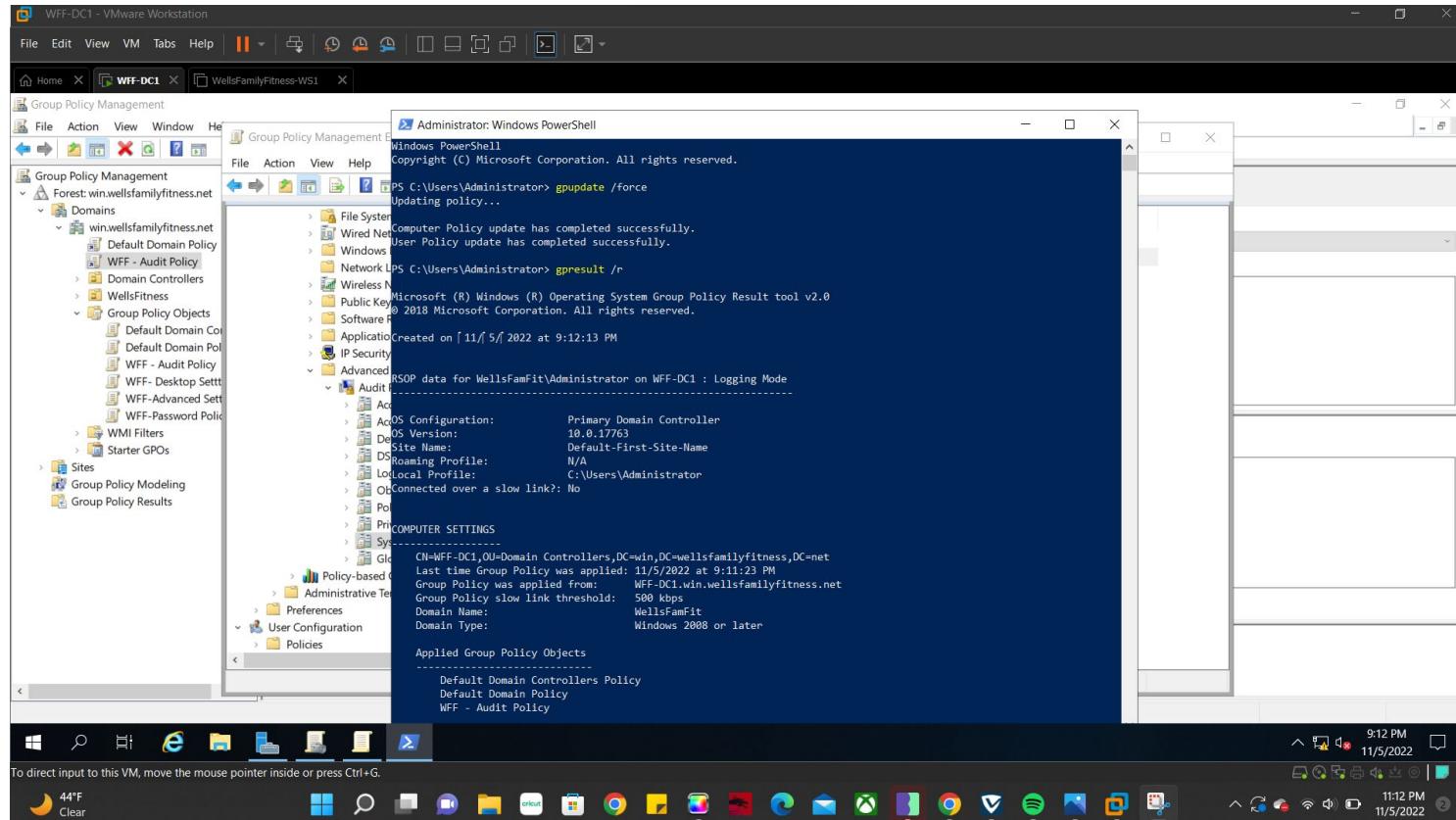
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

44°F Clear

11:10 PM 11/5/2022

This screenshot shows the Group Policy Management Editor window within a VMware Workstation interface. The left pane displays the Group Policy Management structure for the 'Forest: win.wellsfamilyfitness.net' under the 'win.wellsfamilyfitness.net' domain. The 'WFF - Audit Policy' is selected. The right pane shows the 'Audit Other System Events' policy configuration, which is currently set to 'Success and Failure'. The desktop taskbar at the bottom shows various application icons and system status indicators.

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...

The screenshot shows a Windows 10 desktop environment with several windows open:

- Group Policy Management** window (left): Shows the Group Policy Management interface for the forest `win.wellsfamilyfitness.net`. It lists domains like `win.wellsfamilyfitness.net`, group policy objects (GPOs) such as `Default Domain Policy` and `WFF - Audit Policy`, and security groups.
- Administrator: Windows PowerShell** window (center): Displays the results of a command related to Group Policies.

```
The following GPOs were not applied because they were filtered out
-----
Local Group Policy
Filtering: Not Applied (Empty)

The computer is a part of the following security groups
-----
BUILTIN\Administrators
Everyone
BUILTIN\Pre-Windows 2000 Compatible Access
BUILTIN\Users
Windows Authorization Access Group
NT AUTHORITY\NETWORK
NT AUTHORITY\Authenticated Users
This Organization
WFF-DC15
Domain Controllers
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
Authentication authority asserted identity
Denied RODC Password Replication Group
System Mandatory Level

-----
```

USER SETTINGS

```
CN=Administrator,CN=Users,DC=win,DC=wellsfamilyfitness,DC=net
Last time Group Policy was applied: 11/5/2022 at 9:11:24 PM
Group Policy was applied from: WFF-DC1,win.wellsfamilyfitness.net
Group Policy slow link threshold: 500 ms
Domain Name: WellsFamFit
Domain Type: Windows 2008 or later
```

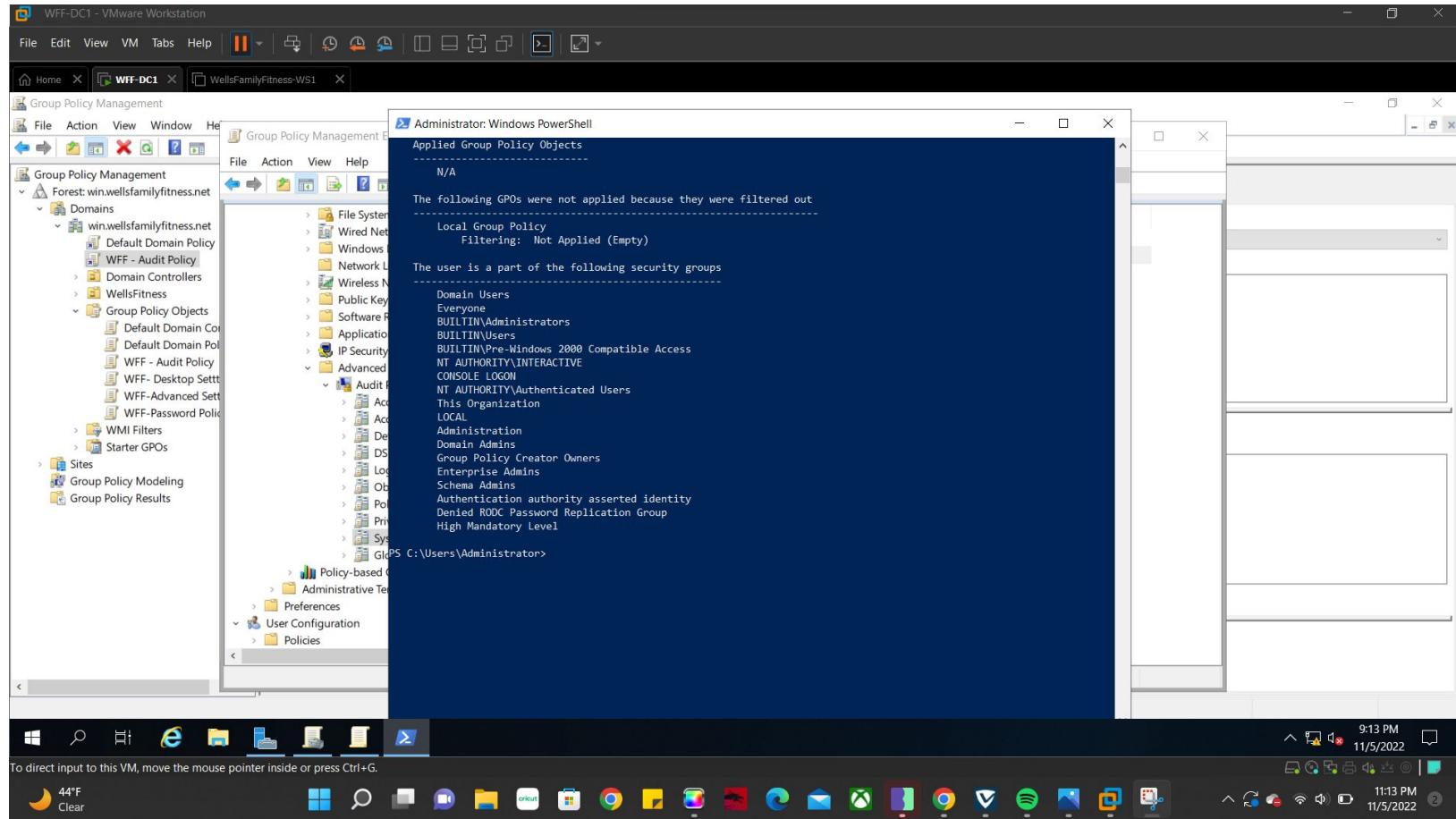
Applied Group Policy Objects

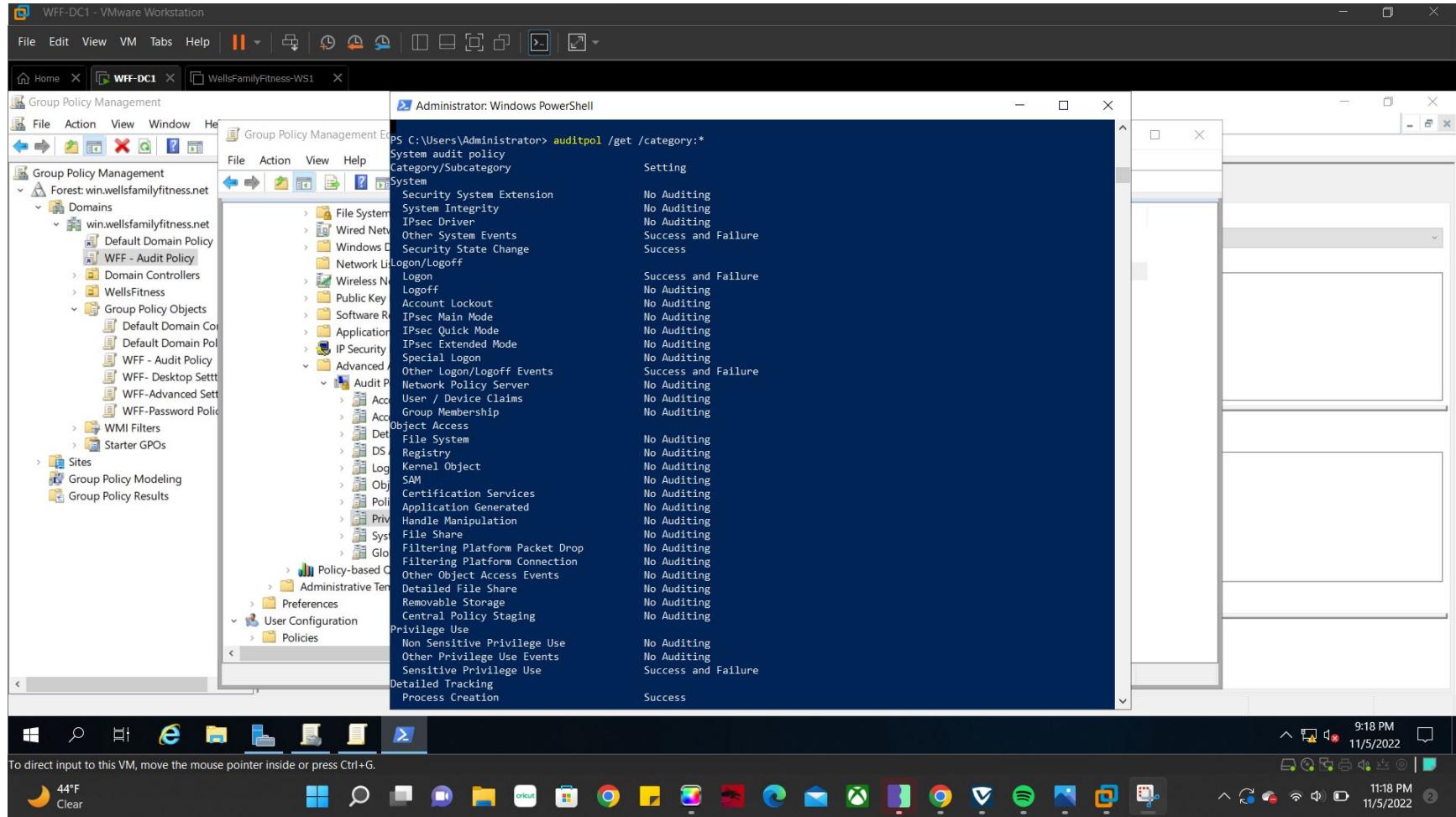
```
M/A
```

The following GPOs were not applied because they were filtered out
-----
Local Group Policy
Filtering: Not Applied (Empty)

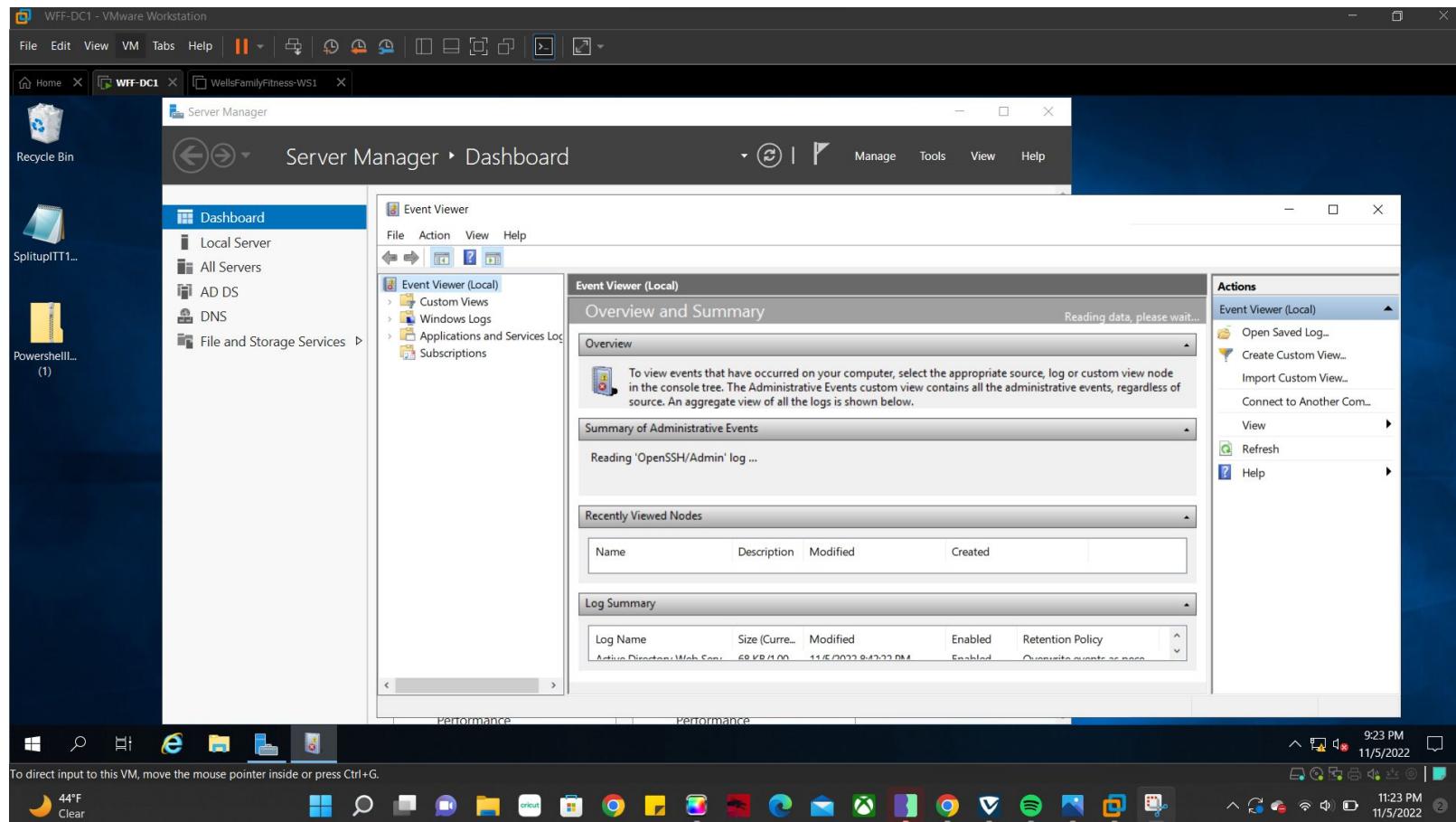
The user is a part of the following security groups
- Taskbar (bottom): Shows the Start button, search icon, task view icon, and pinned icons for File Explorer, Edge, and other applications.
- System tray (bottom right): Shows the date (11/5/2022), time (9:12 PM), battery level, signal strength, and volume controls.

## 17. 15 continued





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

The screenshot shows a Windows desktop environment with a VMware Workstation window titled "WFF-DC1 - VMware Workstation". Inside the window, the Server Manager is open, displaying the Event Viewer. The "Security" log is selected, showing numerous audit events. A specific event, ID 4625, is highlighted in the list, and its properties are shown in a detailed view. The event properties window displays the following information:

General	Details
Account Name: mary	Failure Reason: Unknown user name or bad password.
Account Domain: WellsFamFit	Status: 0xC000006D
	Sub Status: 0xC000006A
Log Name: Security	Logged: 11/5/2022 9:27:43 PM
Source: Microsoft Windows security	Task Category: Logon
Event ID: 4625	Keywords: Audit Failure
Level: Information	User: N/A
User: OpCode: Info	Computer: WFF-DC1.win.wellsfamilyfitness.net
More Information: <a href="#">Event Log Online Help</a>	

The desktop taskbar at the bottom shows various icons, and the system tray indicates the date and time as 11/5/2022 9:30 PM.

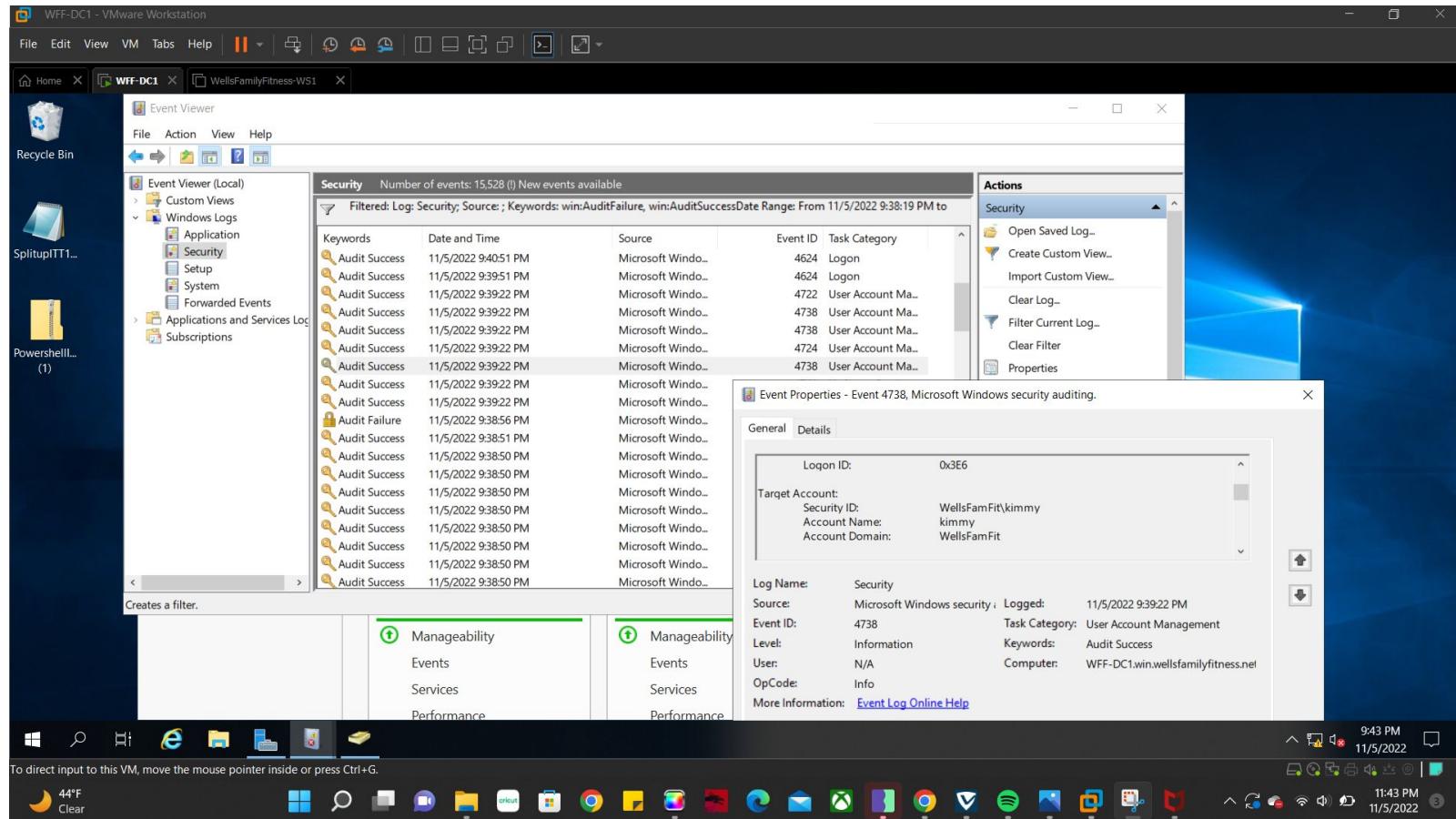
## 21. Go to Active Directory and Computers and create a new user that you will remember

The screenshot shows a Windows desktop environment with several open windows:

- Server Manager**: Shows the "Event Viewer (Local)" pane with "Windows Logs" expanded, displaying categories like Application, Security, System, and Forwarded Events.
- Active Directory Users and Computers**: A table listing users and groups in the domain `win.wellsfamilyfitness.net`. The table includes columns for Name, Type, and Description. Notable users include Cindy, David, Fitness and ..., Healthcare, HR, IT, Jacob, Kimmy, Kristen, Management, Mary, Payroll, Polly, Renee, Retail, Sally, Sarah, Tracy, Warehouse, and Zach.
- Event Viewer**: A context menu is open over an event entry for "Event 4625, Microsoft Window...". The menu options include "Open Saved Log...", "Create Custom View...", "Import Custom View...", "Clear Log...", "Filter Current Log...", "Properties", "Find...", "Save All Events As...", "Attach a Task To This Log...", "View", "Refresh", "Help", "Event Properties", "Attach Task To This Event...", and "Copy".

The taskbar at the bottom shows various pinned icons, including File Explorer, Edge, and several application icons. The system tray shows the date and time as 11/5/2022, 9:39 PM.

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.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Security, Application, Setup, System, Forwarded Events, and Applications and Services Log. The Security log is selected, showing 7,291 events. A specific event, Event ID 4625 (Audit Failure), is highlighted. The right pane contains an 'Actions' menu with options like Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Properties, Find..., Save All Events As..., Attach a Task To This Log..., View, Refresh, Help, Event Properties, Attach Task To This Event..., Copy, Save Selected Events..., Refresh, and Help. Below the main table, a detailed view of Event 4625 is shown, stating 'An account failed to log on.' with Subject: N/A. The event details include Log Name: Security, Source: Microsoft Windows security, Logged: 10/30/2022 11:33:11 PM, Event ID: 4625, Task Category: Logon, Level: Information, Keywords: Audit Failure, User: N/A, Computer: WellsFamFit-WS1.win.wellsfamilyfitness.net, OpCode: Info, and More Information: Event Log Online Help. The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray indicating the date and time as 11:54 PM on 11/5/2022.

WellFamilyFitness-WS1 - VMware Workstation

File Edit View VM Tabs Help

Event Viewer

File Action View Help

Event Viewer (Local)

Keywords Date and Time Source Event ID Task Category

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	11/5/2022 11:50:35 PM	Microsoft Windows security auditing.	4688	Process Creation
Audit Success	11/5/2022 11:50:34 PM	Microsoft Windows security auditing.	4688	Process Creation
Audit Success	11/5/2022 11:50:34 PM	Microsoft Windows security auditing.	4826	Other Policy Change Events
Audit Success	11/5/2022 11:50:34 PM	Microsoft Windows security auditing.	4690	Process Creation
Audit Success	11/5/2022 11:50:34 PM	Microsoft Windows security auditing.	4688	Process Creation
Audit Success	11/5/2022 11:50:38 PM	Eventlog	1101	Event processing
Audit Success	10/30/2022 11:33:54 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	10/30/2022 11:33:54 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	10/30/2022 11:33:53 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	10/30/2022 11:33:53 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	10/30/2022 11:33:46 PM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	10/30/2022 11:33:12 PM	Microsoft Windows security auditing.	4799	Security Group Management
Audit Success	10/30/2022 11:33:11 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	10/30/2022 11:33:11 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	10/30/2022 11:33:11 PM	Microsoft Windows security auditing.	4648	Logon
<b>Audit Failure</b>	<b>10/30/2022 11:33:11 PM</b>	<b>Microsoft Windows security auditing.</b>	<b>4625</b>	<b>Logon</b>
Audit Success	10/30/2022 11:32:51 PM	Microsoft Windows security auditing.	4799	Security Group Management
Audit Success	10/30/2022 11:32:51 PM	Microsoft Windows security auditing.	4799	Security Group Management
Audit Success	10/30/2022 11:32:51 PM	Microsoft Windows security auditing.	4634	Logoff

Event 4625, Microsoft Windows security auditing.

General Details

An account failed to log on.

Subject:

Log Name: Security  
Source: Microsoft Windows security  
Logged: 10/30/2022 11:33:11 PM  
Event ID: 4625  
Task Category: Logon  
Level: Information  
Keywords: Audit Failure  
User: N/A  
Computer: WellsFamFit-WS1.win.wellsfamilyfitness.net  
OpCode: Info  
More Information: Event Log Online Help

Creates a filter.

Type here to search

11:54 PM 11/5/2022

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

44°F Clear

11:54 PM 11/5/2022