Configuring a System for Auditing Policies

(CompTIA Security + SY – 601)

Objective(s):

- To implement identity and account management controls

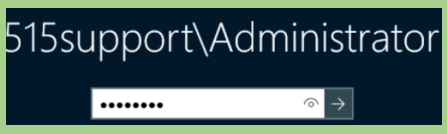
Resources:

- Windows Virtual Machine (DC1)
- Command-line tools

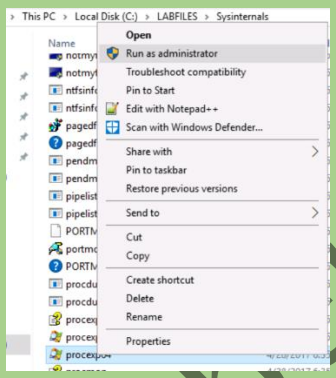
Instructions:

Browse running processes

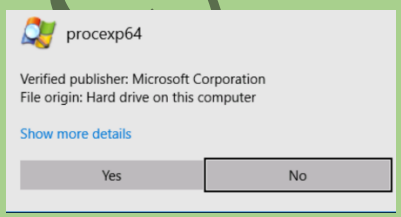
- Log-in to DC1 VM



- Open File Explorer and browse to C:\LABFILES\Sysinternals

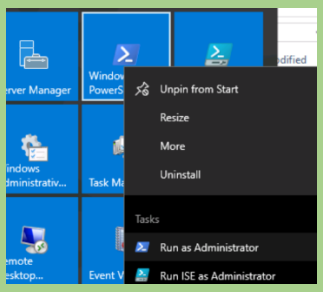


- Right-click **procexp64.exe** and select **Run as administrator**. Select **Yes** at the UAC prompt



- Close the Process Explorer window. Minimize the File Explorer window

- From the **Start** menu, right-click **Windows PowerShell** and then select Run as **Administrator**. Select Yes to confirm the UAC prompt



- Enter the following command to generate similar information: **tasklists**

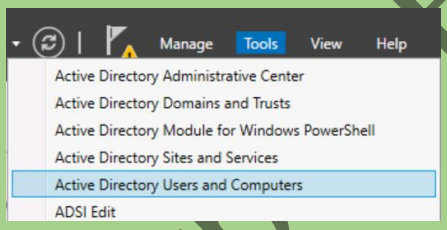
```
PS C:\Windows\system32> tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          4 K
System                           4 Services                   0        140 K
smss.exe                       268 Services                   0      1,240 K
csrss.exe                      364 Services                   0      4,416 K
csrss.exe                      432 Console                    1      5,512 K
wininit.exe                    444 Services                   0      4,872 K
```

- Run the tasklist command again, and this time filter for running services. Redirect the output of the command to a **text.file** named **C:\services.running.txt**

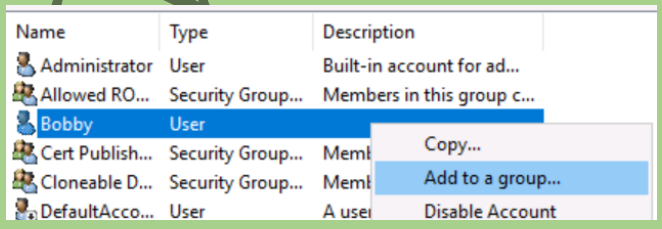
```
PS C:\Windows\system32> tasklist /SVC /FI "STATUS eq RUNNING" > C:\services-running.txt
```

Auditing effective permissions

- In Server Manager, select **Tools**, and then select **Active Directory Users and Computers**

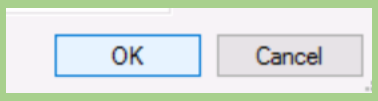


- Select the **Users** container, right-click the **Bobby** account, and select **Add to a group**

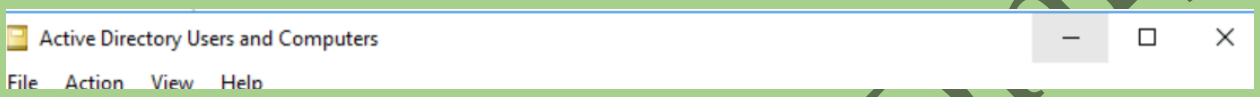


- Enter **Sales** and then select Check Names

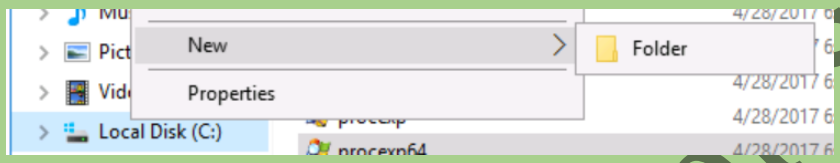
- Select **OK** to confirm both dialog boxes



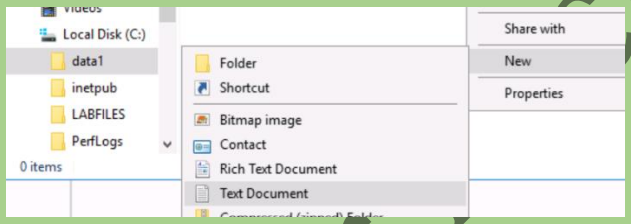
- Minimize **Active Directory Users and Computers open**



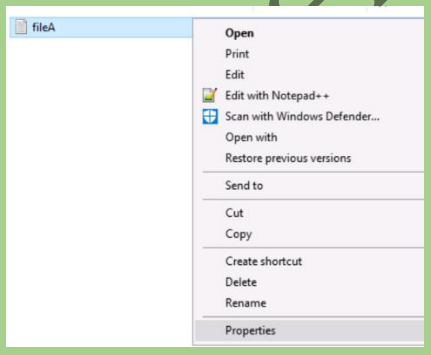
- In the File Explorer, right-click C:\and create a folder named **data1**



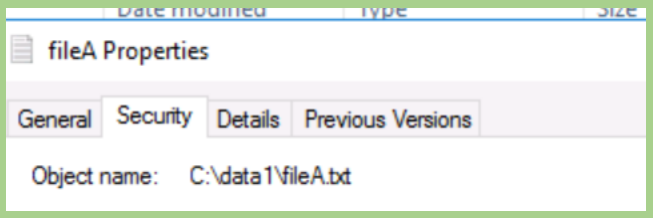
- Select the data1folder. Right-click within the folder and select **New > Text Document**. Enter the name **fileA** and press Enter



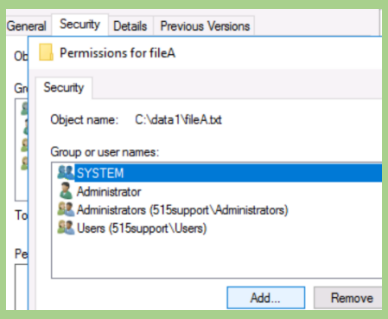
- Right-click the **C:\data1** folder, and then select **Properties**



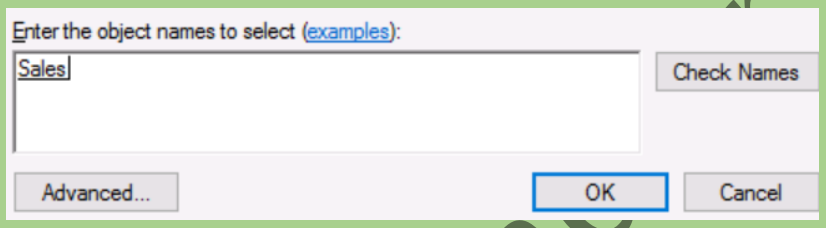
- Select the **Security** tab to configure NTFS permissions



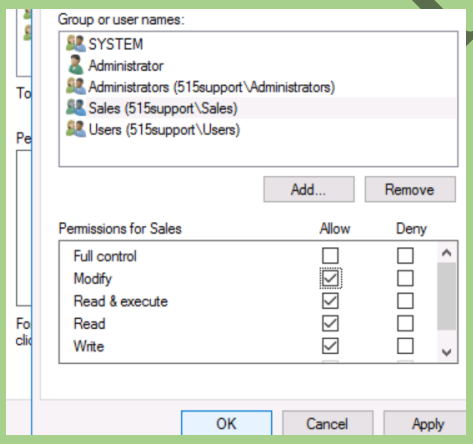
- On the Security tab, select the **Edit** button. In the Permissions for data1 dialog box, select **Add** button



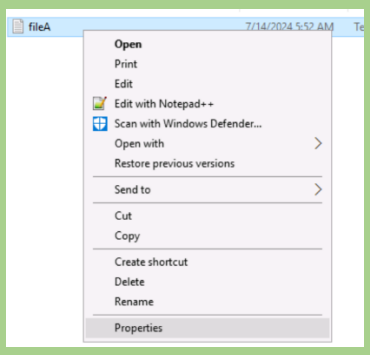
- Type **Sales**, and then select the **Check Names** button, select **OK**



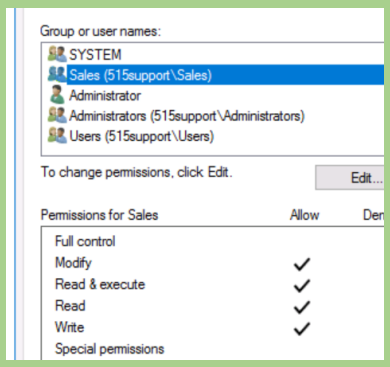
- With the **Sales** group highlighted in the Permissions for data1 dialog box, select the **Modify** check box in the Allow column. Select **OK** to confirm each dialog box



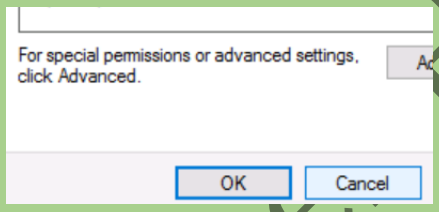
- In C:\data1, right-click **fileA.txt** and then select **Properties**



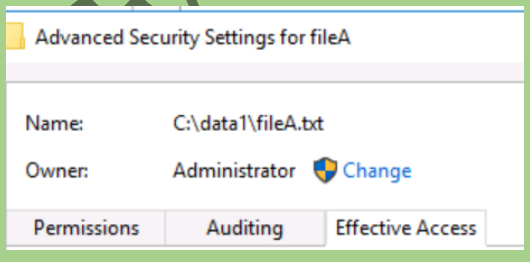
- On the **Security tab**, observe that the **Sales** group is listed



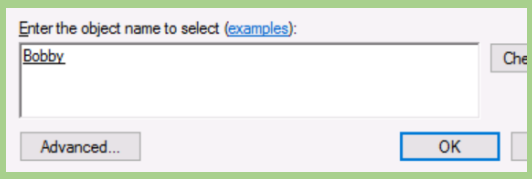
- Select **Cancel** to close the fileA.txt Properties box



- In the File Explorer, right-click the **C:\data1** folder, select **Properties**, select the **Security tab**, and then select the **Advanced** button

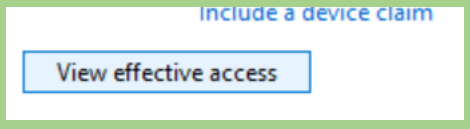


- Select the **Effective Access** tab

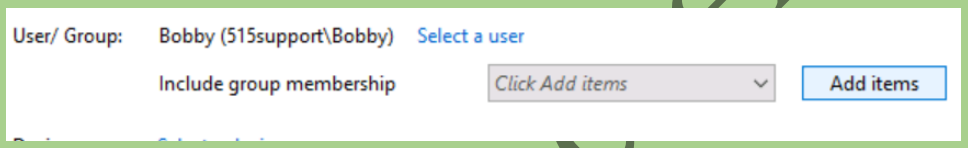


- In the **Select a user interface**, enter **Bobby**, select **Check Names** and then select **OK**

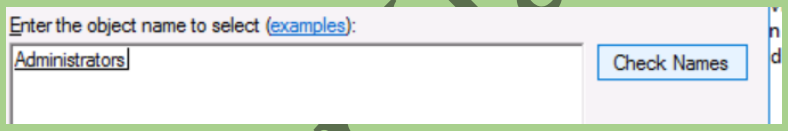
- Select **view effective access** and note the permissions



- In the interface, at **include a group membership**, select **Add items**

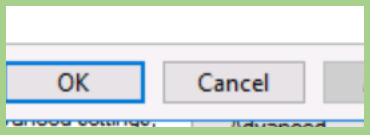


- Enter **Administrators**, select **Check Names** and then select **OK**



- Select **View effective access** again

- Select **Cancel** to exit each dialog box. Close Filer Explorer

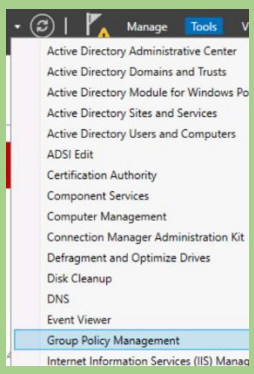


- Run the following Powershell cmdlet to display permissions information for **fileA.txt**

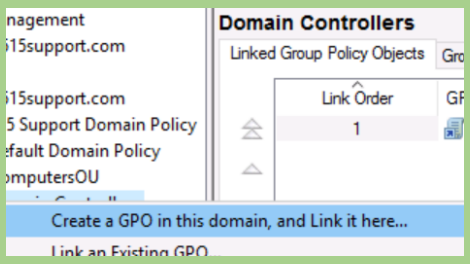
```
PS C:\Windows\system32> get-acl C:\data1\fileA.txt | format-list | out-file C:\permissions.txt
```

Create file systems audit policy

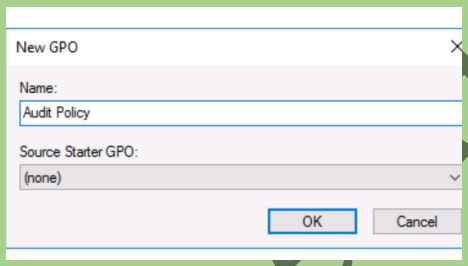
- In Server Manager, Select Tools and then select the **Group Policy Management** console



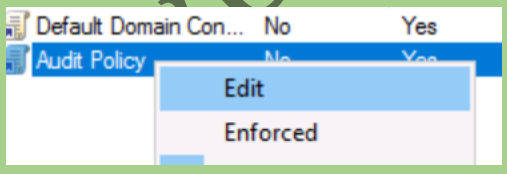
- In the Group Policy Management console, select the **Domain Controllers** organizational unit, Right-click it and select, **Create a GPO in this domain**, and **Link it here**



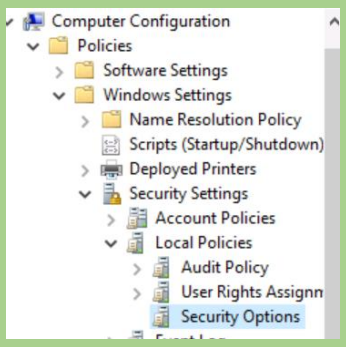
- In the Name box, enter **Audit Policy** and select **OK**



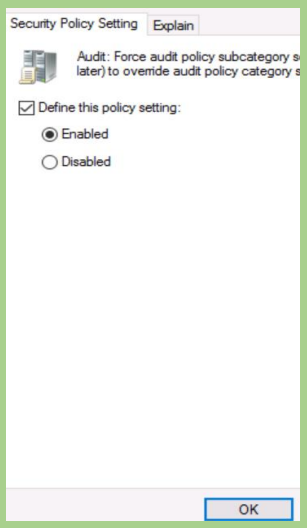
- Right-click **Audit Policy** and select **Edit**



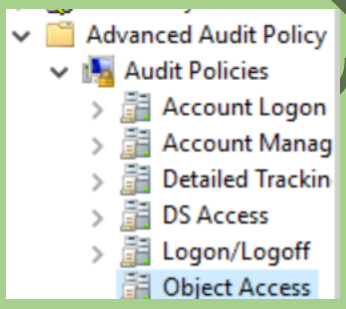
- In the Group Policy Management Editor console expand **Computer Configuration > Policies > Window Settings > Security Settings > Local Policies > Security Options**



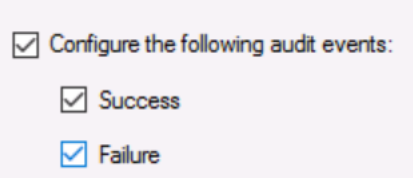
- Select Audit: **Force audit policy subcategory settings.** Check the **Define this policy settings** check box and select the **Enabled** option button. Select OK



- In the Group Policy Management Editor console, expand **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Object Access**



- Double-click **Audit File System**. Check the **Configure the following audit events** check box, and then check the boxes for both **Success** and **Failure**



- Select **OK** to close the interface
- In the elevated PowerShell console. Run the following command to immediately apply the new GPO to the Domain Controllers Organizational Unit: **gpupdate**

```
PS C:\Windows\system32> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
```

GPO reporting

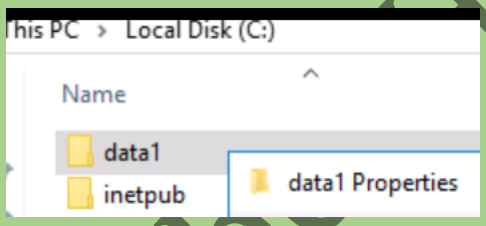
- Run the following command to create a file containing the applied Group Policy settings: **gpresult \H C:\audit.html**

```
PS C:\Windows\system32> gpresult /H C:\audit.html
```

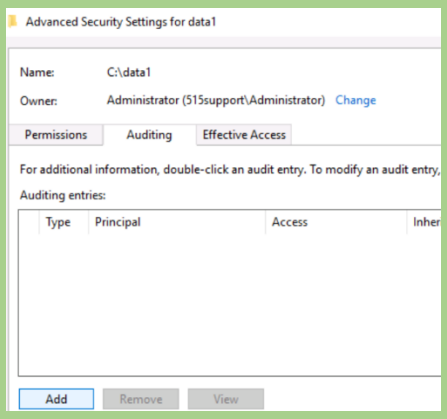
- Close the Group Policy Management Editor window

Display audit policy results by using Event Viewer

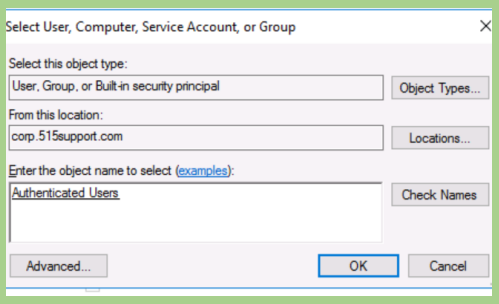
- In the File Explorer, right-click the C:\data1 folder and select **Properties**



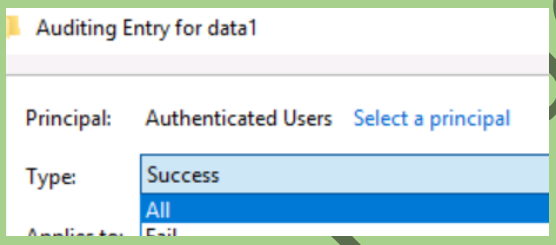
- In the data1 Properties dialog box, select the **Security** tab, and then select the **Advanced** button
- On the **Auditing** tab, select **Continue** and then select **Add**



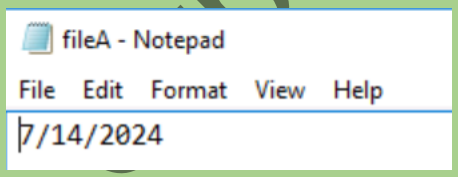
- Select the Select a principal link, and in the Select User, Computer, Service Account, or Group box, type **Authenticated Users** and select **OK**



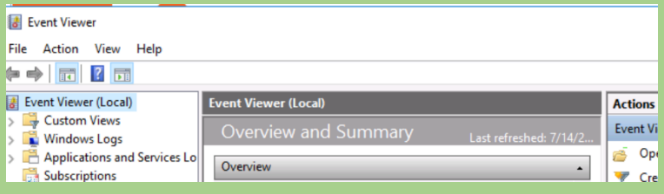
- Set the **Type** of audit at **All** from the pull-down menu



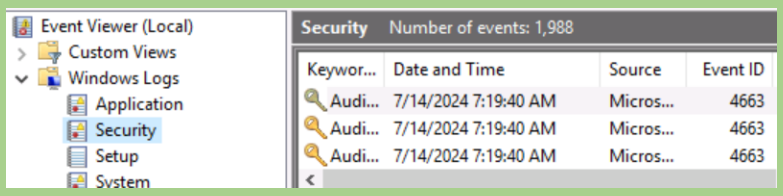
- Select **OK** to confirm each dialog box
- Open C:\data1\fileA.txt, add today's data to the file, and then save and close it



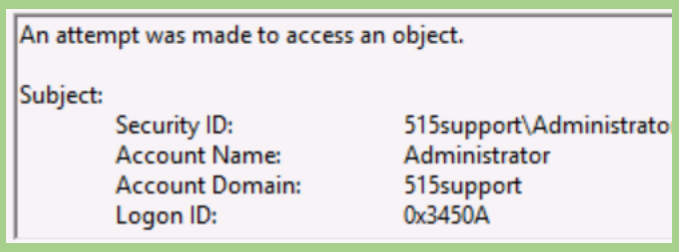
- From Server, Manager, select **Tools** and then select **Event Viewer**



- Expand the **Windows Logs** node, and then select the **Security** log.



- Select the event at the top of the list



Observation:

- The Sales group was correctly assigned Modify permissions on the specified folder and file.
- Effective permissions were accurately verified for user Bobby.
- Audit policies were enabled and confirmed through event logs.

Results:

- Successfully configured and applied NTFS permissions to the Sales group.
- Created and linked a Group Policy Object (GPO) for auditing.
- Verified audit settings through Event Viewer logs.

Future Work:

- Explore automated scripts for regular auditing policy updates.
- Implement real-time alerts for unauthorized access attempts.
- Extend auditing to other critical system areas and resources.