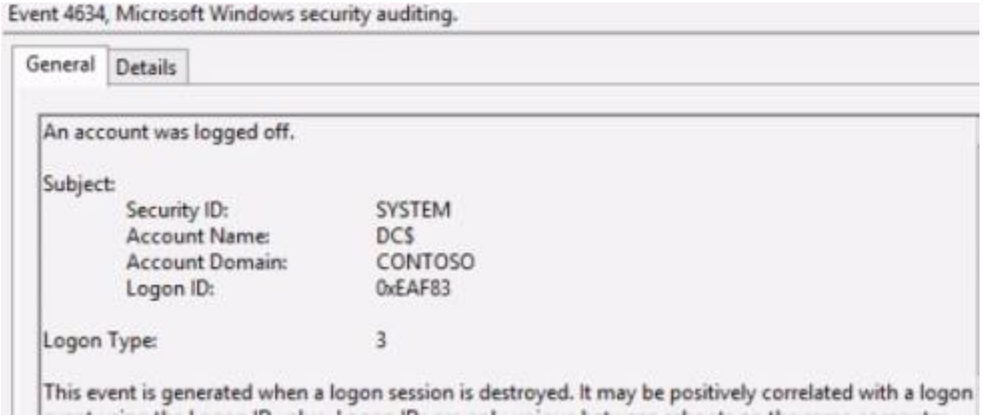
Security Audit policy lab notes

Click on Next to begin your lab Exercise

1. In Server Manager click on Tools, **Event Viewer**
2. In Event Viewer click on **Windows Logs**, then click on **Security**
3. Notice that the first Event, ID 4634, is highlighted
4. Look below at the Details pane, notice the details



Event 4634, Microsoft Windows security auditing.

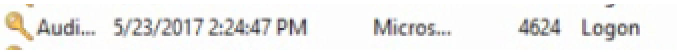
An account was logged off.

Subject:
    Security ID: SYSTEM
    Account Name: DC$
    Account Domain: CONTOSO
    Logon ID: 0xEAF83

Logon Type: 3

This event is generated when a logon session is destroyed. It may be positively correlated with a logon

5. Select Event ID 4624, 2:24 pm



Audi... 5/23/2017 2:24:47 PM Micros... 4624 Logon

6. Notice the Details in the pane below
7. Close the Event View box.

Configure Audit Policy Object Access

1. In Server Manager click on Tools, Group Policy Management
2. In Group Policy Management, expand contoso.com,
3. Right-click on Group Policy Objects, then click on New
4. Type **audit for sales data** for the name of the GPO, then press **Enter**
5. On the New GPO dialog box click **OK**
6. In Group Policy Management Expand **Group Policy Objects**
7. Right-click on the GPO **audit for sales data,** then click on **Edit**
8. Select **Computer configuration, Policies, Windows Settings, Security Settings, Local Policies, Audit Policies**
9. Select **Audit Object Access**
10. In **Object Access Properties** Box, select **Define these policy settings**, Select **Success**, Select **Failure**
11. Click on the **Explain** tab**,** pay attention to the explanation, click on OK to close the box
12. Close Group Policy Management Editor, Close Group Policy Management

Turning on audit on the Sales Data Folder

1. On the task bar click on **File Explorer** icon

2. Click on **Local Disk C:**
3. Right-click on **Sales Data** and click on **Properties**
4. On the Sales Data Properties box click on **Security** then click on **Advanced**
5. Click on **Auditing ,** click on **Add**
6. On the **Audit Entry for sales data** dialog box Click on **Select a Principal**
7. Select **Advanced, Find Now**
8. Select **Ben Smith**
9. Click on **OK** 4 times
10. Close the Sales Data Properties box
11. Close **Local Disk C:**

Editing the GPO to look at other Audit policies

1. Click on **Tools**, **Group Policy Management**
2. Expand **contoso.com**
3. Expand **Group Policy Objects**
4. Right click on **audit for sales data** and click **Edit**
5. Select **Computer configuration, Policies, Windows Settings, Security Settings, Local Policies, Audit Policies**
6. Select **Audit Account Logon Events**
7. Select **Define these Policy Settings,** then click on the Explain tab. Read the explanation
8. Close the **Audit Account Logon Events** properties box
9. Select **Audit account management**
10. Select **Define these Policy Settings,** Select **Failure,** Select **Success,** then click on the Explain tab
11. Read the explanation then close the box
12. Click on Audit directory service access
13. Select **Define these Policy Settings,** Select **Success,** then click on the Explain tab, then close the properties box
14. Select **Audit logon events,** Select **Define these Policy Settings,** click on the Explain tab, Read the explanation then close the box
15. Click on audit Policy Change , Select **Define these Policy Settings,** Click on success then click on the Explain tab, Read the explanation then close the box
16. Click on Audit System Events, Select **Define these Policy Settings,** Click on success then click on the Explain tab, Read the explanation then close the box
17. Click on Audit Process Tracking, Select **Define these Policy Settings,** Click on Failure then click on the Explain tab, Read the explanation then close the box
18. Click on Audit privilege use, Select **Define these Policy Settings,** Click on success then click on the Explain tab, Read the explanation.

End of Lab*