Lab Objective

Learn how to use AuditPol.exe

**Lab Procedures**

**1.** On the RWDC01 server, open a Command Prompt, and execute the following command to get a list of all Audit settings:

auditpol /get /category:\*

**2.** To see the audit policy set for Contoso\User1, execute the following command:

auditpol.exe /get /user:contoso\user1 /category:\*

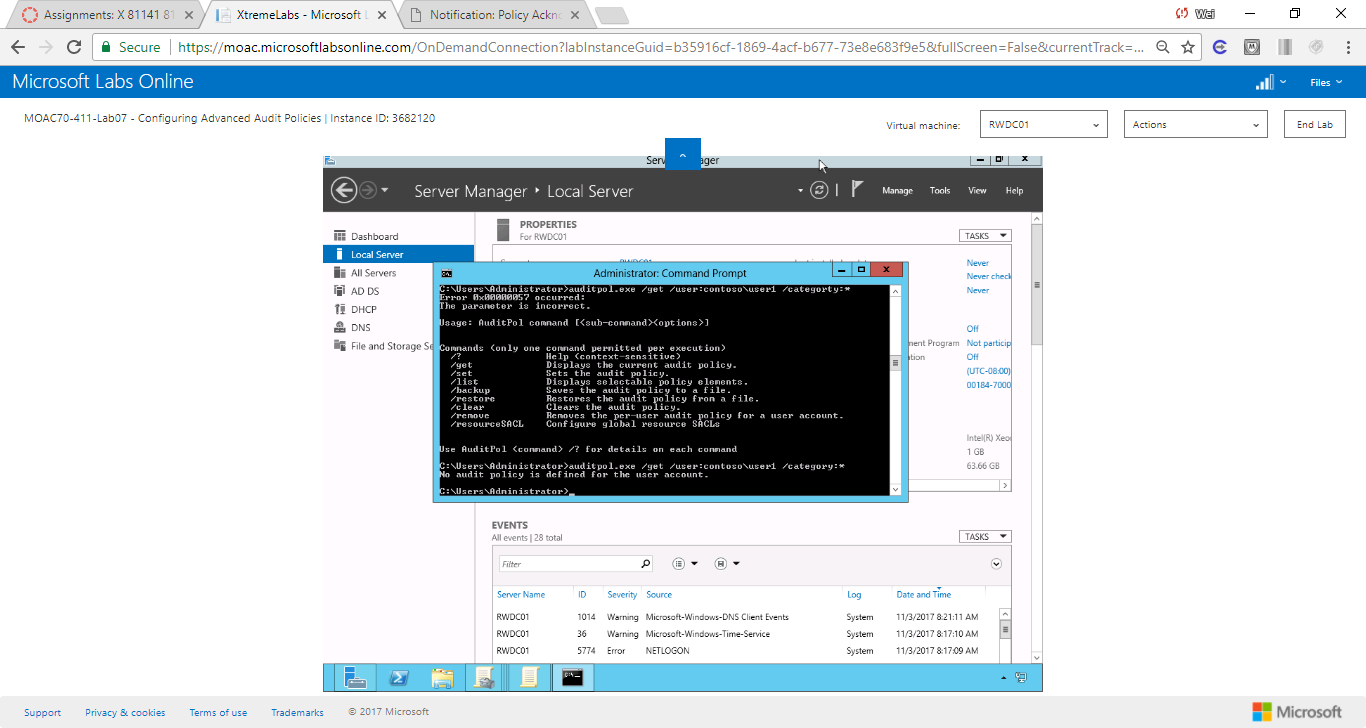


Figure 1 Observe that there is no audit policy defined for Contoso\User1

**3.** Observe that there is no audit policy defined for Contoso\User1. To set the audit policy for User1 so that account management is audited for User1, execute the following command:

auditpol.exe /set /user:contoso\user1 /subcategory:"user account management" /success:enable /failure:enable

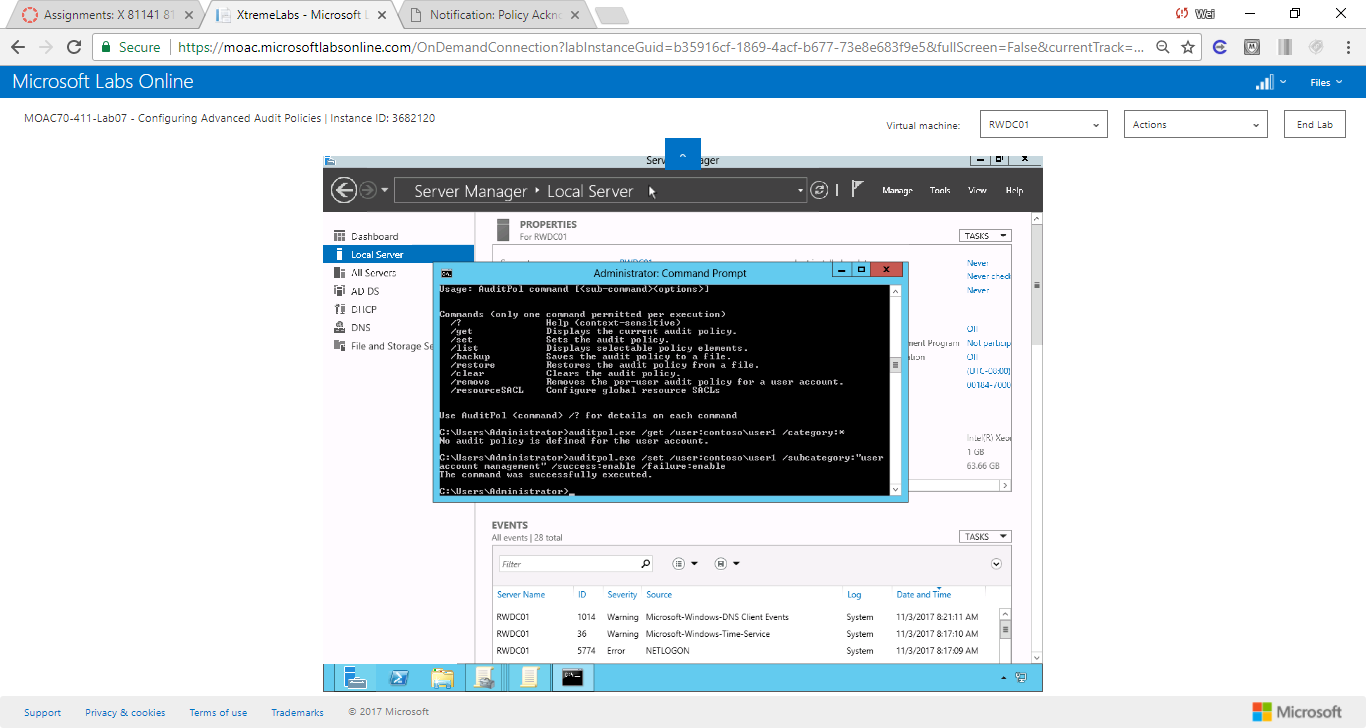


Figure 2 The command was successfully executed.

**4.** To display the settings for everyone again, run the following command:

auditpol /get /category:\*

**5.** To get the settings for user1, execute the following settings:

auditpol.exe /get /category:\* /user:user1

|  |  |
| --- | --- |
| Question 5 | Are the audit policies configured with Group Policies displayed when you specified a single user? Yes |

**6.** Take a screen shot of the Command Prompt window by pressing Alt+Prt Scr and then paste it into your Lab07\_worksheet file in the page provided by pressing Ctrl+V.

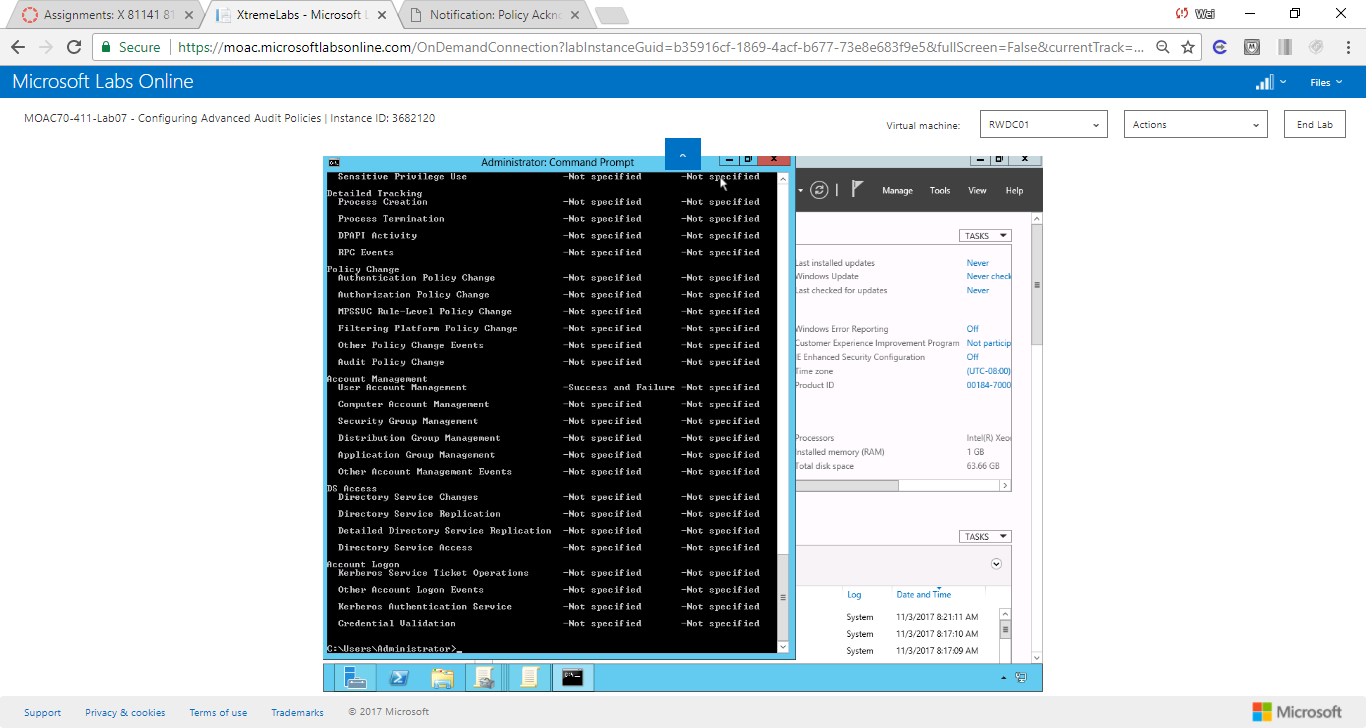


Figure 3 settings for user1

**7.** To reset the settings for user1, execute the following settings:

auditpol /remove /user:contoso\user1

**8.** Verify that the per-user setting was removed by running the following command:

auditpol.exe /get /user:contoso\user1 /category:\*

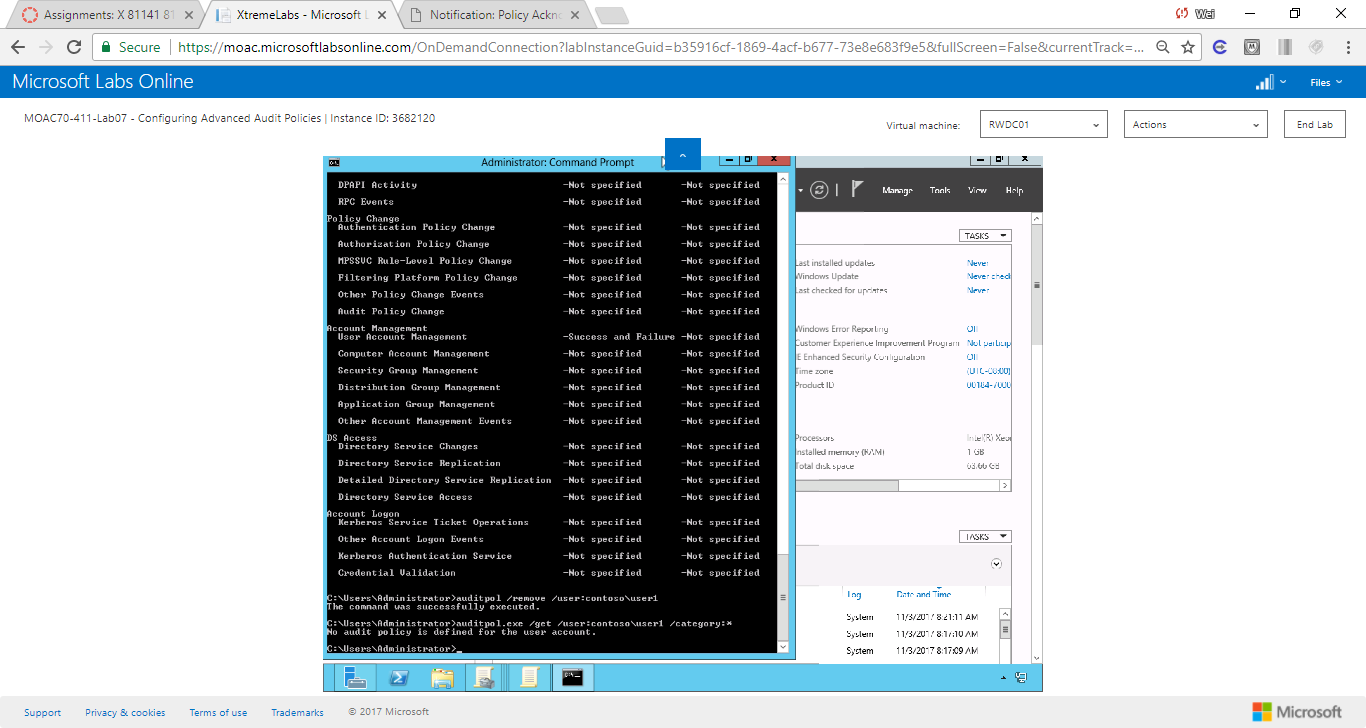


Figure 4 The per-user setting was removed.

**Lab Summary**

During this exercise, I used AuditPol.exe to manage auditing. Auditpol.exe is command based which is faster to manipulate the settings than advanced audit policies. I used the following command to configure a user-based audit policy.

auditpol.exe /set /user:contoso\user1 /subcategory:"user account management" /[options]