CST223 M07 Assignment – 7.2 GPMgmt
Wei Cui 11/03/2017

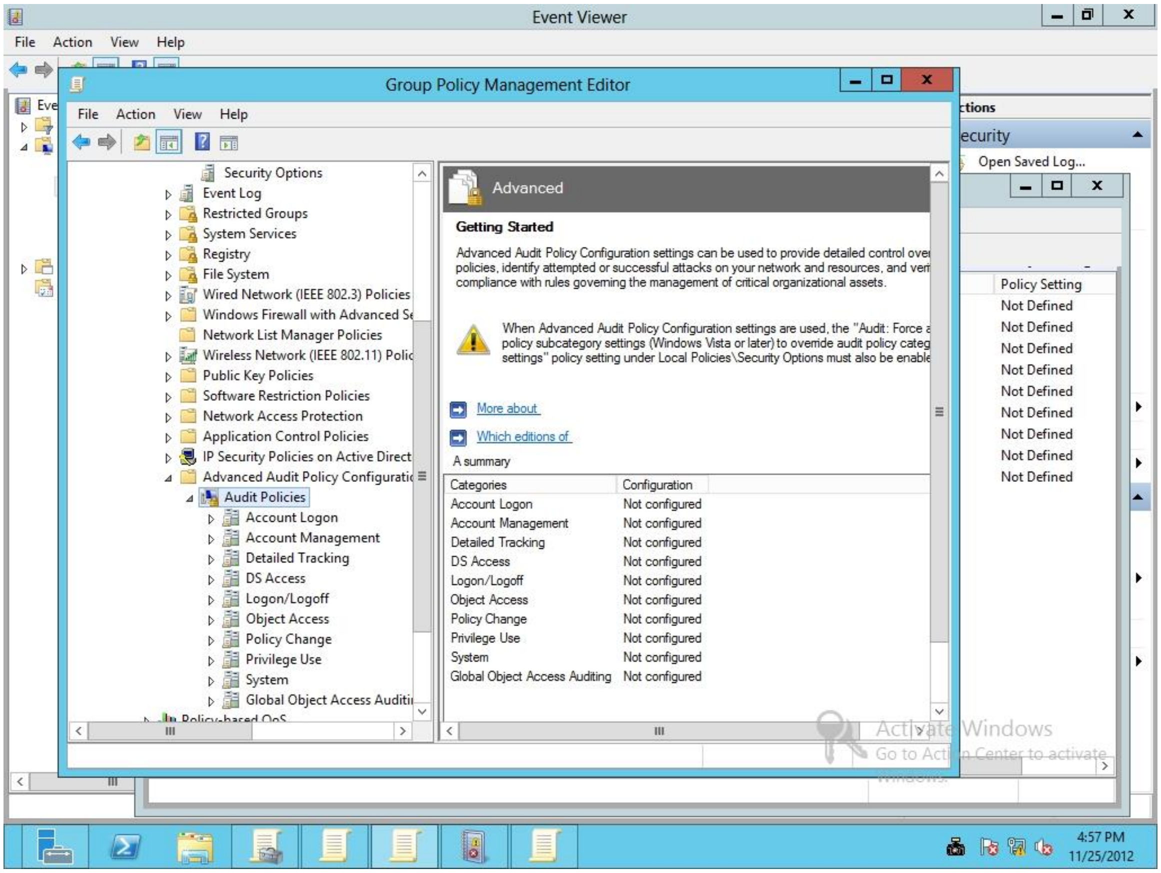
Lab Objective

Implementing Advanced Auditing

Lab Procedures

1. On the RWDC01 server, if the Group Policy Management Editor is not open for the Audit Policy policy, right-click the Audit Policy and click Edit.

2. In the Group Policy Management Editor on RWDC01, navigate to Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration and click Audit Policies, as shown in Figure 7-3.



Getting Started

Advanced Audit Policy Configuration settings can be used to provide detailed control over policies, identify attempted or successful attacks on your network and resources, and veri compliance with rules governing the management of critical organizational assets.

When Advanced Audit Policy Configuration settings are used, the "Audit: Force a policy subcategory settings (Windows Vista or later) to override audit policy categ settings" policy setting under Local Policies\Security Options must also be enable

More about

Which editions of

A summary

Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured
Global Object Access Auditing	Not configured

Figure 7-3
Configuring Advanced Audit Policy configuration settings

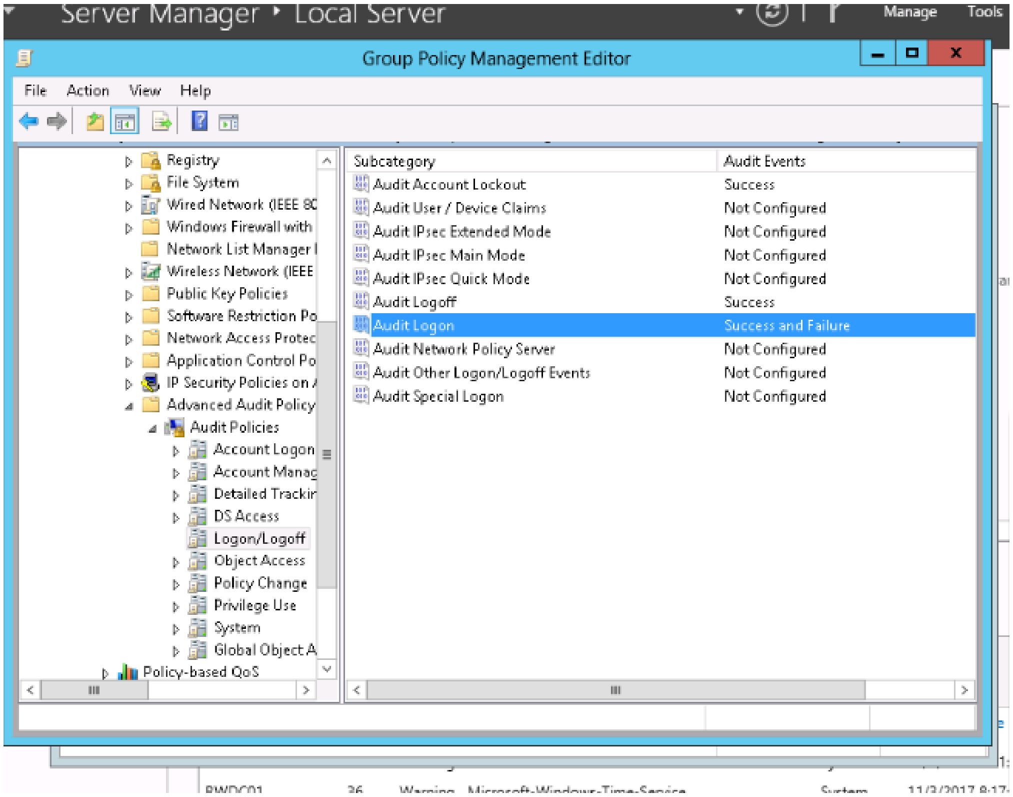
3. Under Audit Policies, double-click Logon/Logoff.

4. Double-click Audit Account Lockout. When the Audit Account Lockout Properties dialog box opens, click to select Configure the following audit events, and then select Success. Click OK to close Audit Lockout Properties.

5. Configure the following settings:

Audit Logoff	Success
Audit Logon	Success and Failure

6. Take a screen shot of the Group Policy Management Editor window by pressing Alt+Prt Scr and then paste it into your Lab07_worksheet file in the page provided by pressing Ctrl+V.



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

Figure 1 A screen shot of the Group Policy Management Editor window after Step 1- 5

7. Under Audit Policies, click Account Management and configure the following settings:

Audit Computer Account Management	Success and Failure
Audit Security Group Management	Success and Failure
Audit User Account Management	Success and Failure

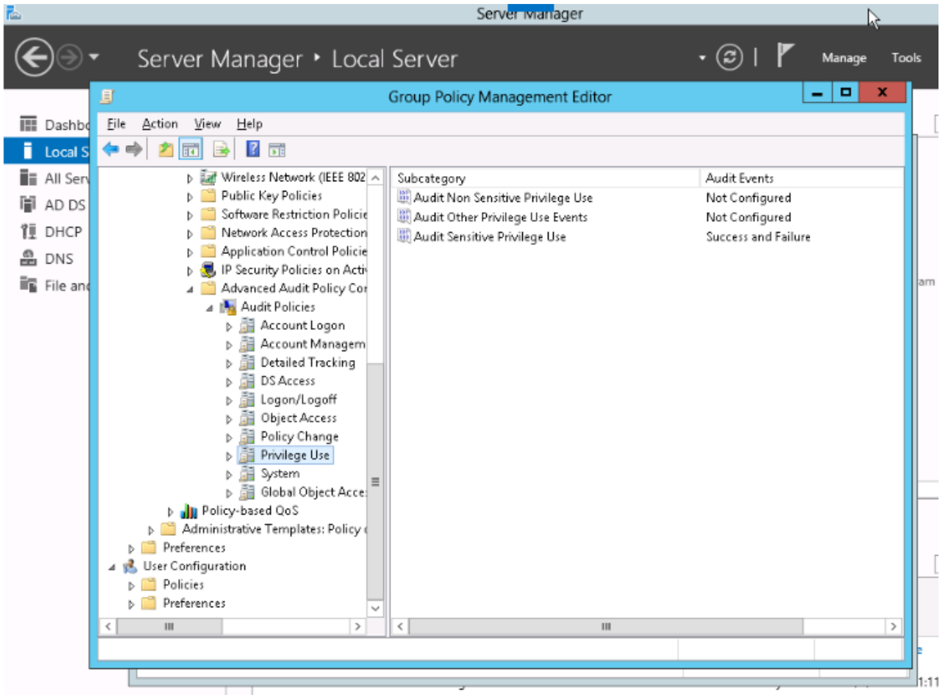
8. Under Audit Policies, click Object Access and configure the following settings:

Audit File Share	Success and Failure

Audit File System	Success and Failure
Audit Registry	Success and Failure
Audit SAM	Success and Failure

9. Click Privilege Use and configure the following settings:

Audit Sensitive Privilege Use	Success and Failure

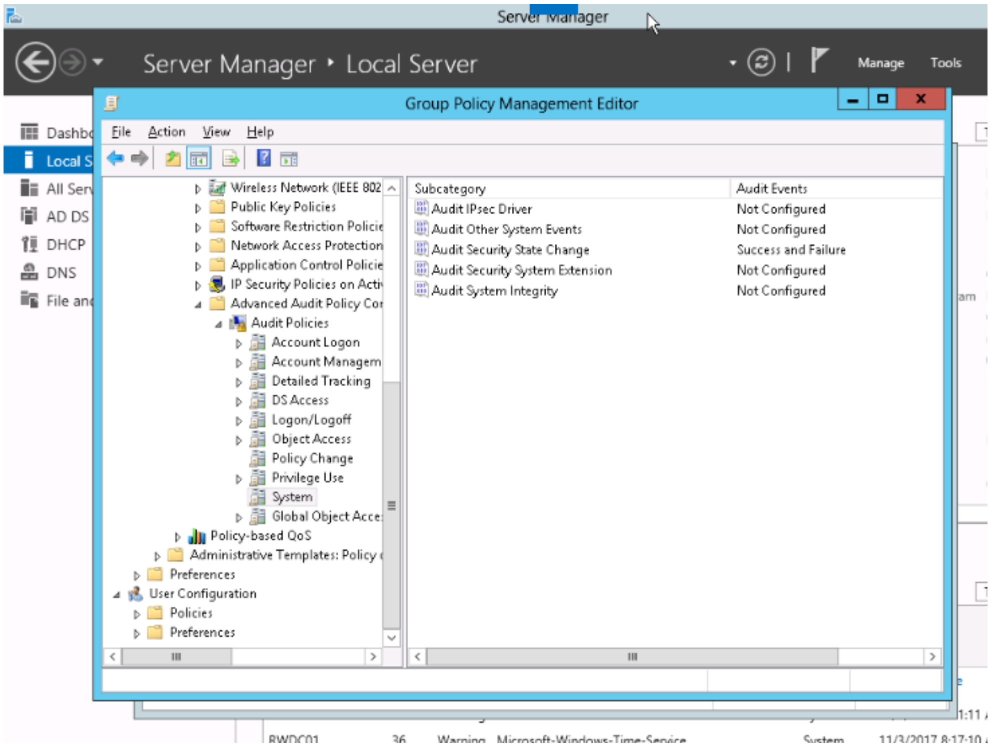


Subcategory	Audit Events
Audit Non Sensitive Privilege Use	Not Configured
Audit Other Privilege Use Events	Not Configured
Audit Sensitive Privilege Use	Success and Failure

Figure 2 Privilege User Configuration

10. Click System and configure the following settings:

Audit Security State Change	Success and Failure

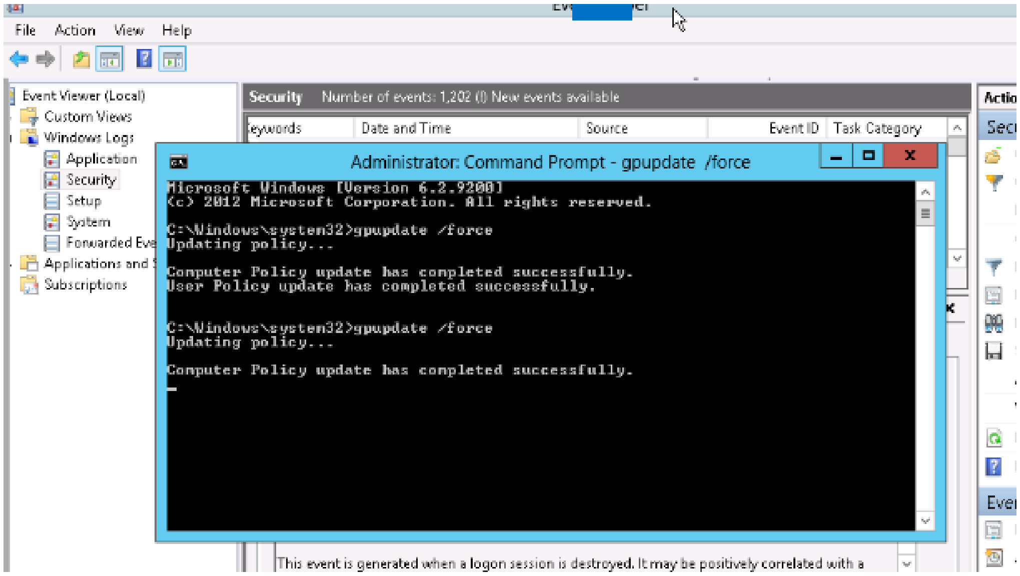


Subcategory	Audit Events
Audit IPsec Driver	Not Configured
Audit Other System Events	Not Configured
Audit Security State Change	Success and Failure
Audit Security System Extension	Not Configured
Audit System Integrity	Not Configured

Figure 3 Screenshot of System Configuration

11. Close the Group Policy Management Editor.

12. Go to Server01, open a Command prompt windows, and execute the `gpupdate /force` command.



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

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

Computer Policy update has completed successfully.
User Policy update has completed successfully.


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

Computer Policy update has completed successfully.
_
```

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

Figure 4 gpupdate command was executed successfully.

CST223   M07 Assignment – 7.2 GPMgmt
Wei Cui   11/03/2017

Lab Summary

During this exercise, I used Advanced Audit Policies to help keep track of who uses and attempts to use my network resources. Advanced auditing have more options to aduit than standard auditing. Advanced auditing settings is located here

> *In the Group Policy Management Editor on RWDC01, navigate to Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration*

I can enable auditing of the Registry Under Audit Policies, click Object Access, audit registry.