Advanced Audit Policy Configurations for LT Auditor+

Reference Guide

Contents

WINDOWS AUDIT POLICIES REQUIRED FOR LT AUDITOR+.

SACL's need to be configured, to audit Active Directory, File System and Login/Logout events, on the Windows system. The following sections detail the specific policies required for Advanced Audit policies on Windows 2008R2/Windows 2012 systems.

ACTIVE DIRECTORY

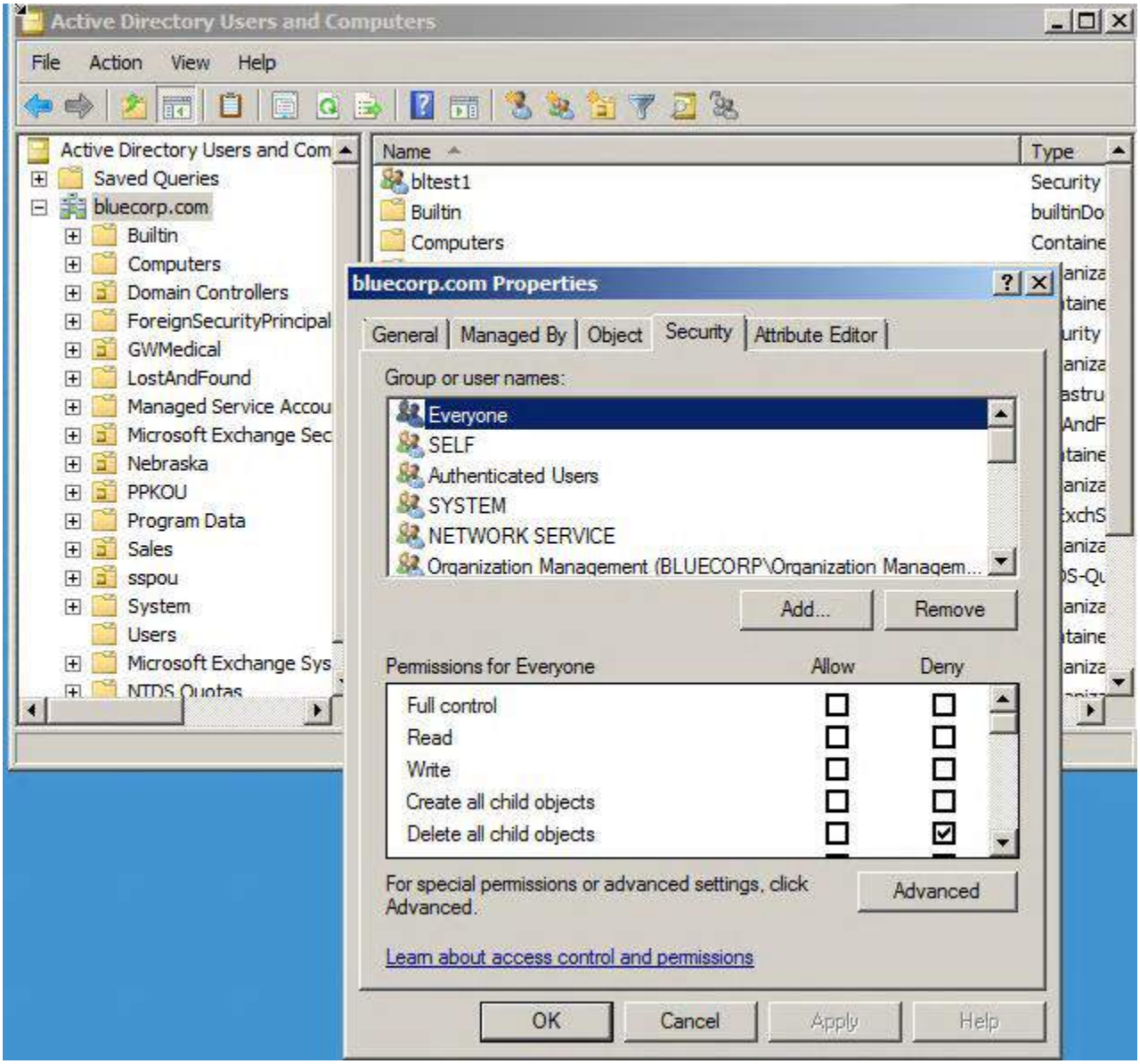
To successfully audit Active Directory events, with LT Auditor+, the following SACL's (Security Access Control Lists) need to be configured.

1. Audit Policy(SACL) for the Domain Object
2. Advanced Audit Policy for the Default Domain Controller Group Policy

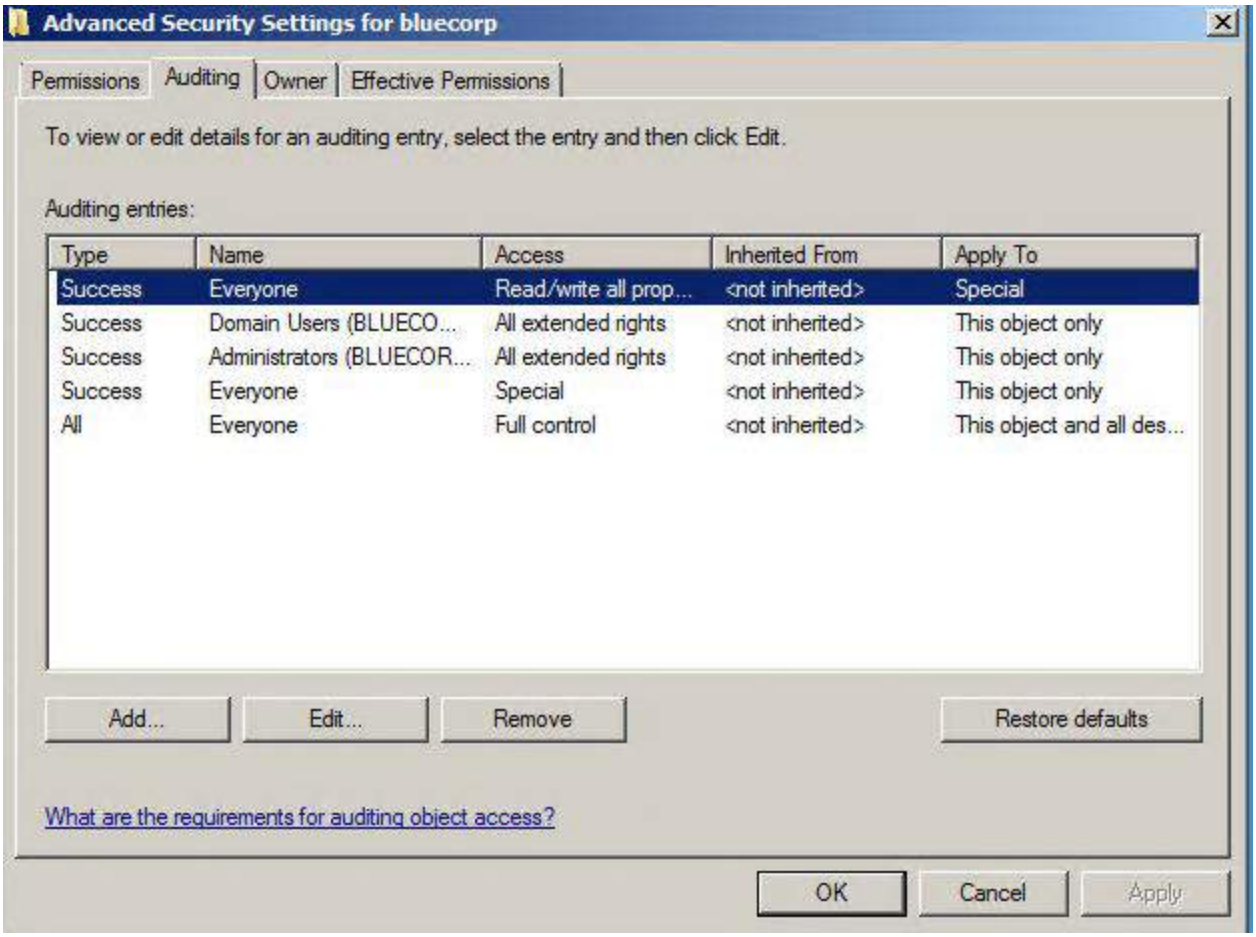
Audit Policy for the Domain

This setting may be configured by default, but it is important to validate that the following audit entries are defined on the Domain object.

1. Launch Windows Active Directory and Users MMC.
2. Click on View → Advanced Features to enable
3. Right-Click on the root Domain object and click on Properties to bring up the Properties Window as shown below



4. Select the Security Tab and click on Advanced and select the Auditing tab as shown below:

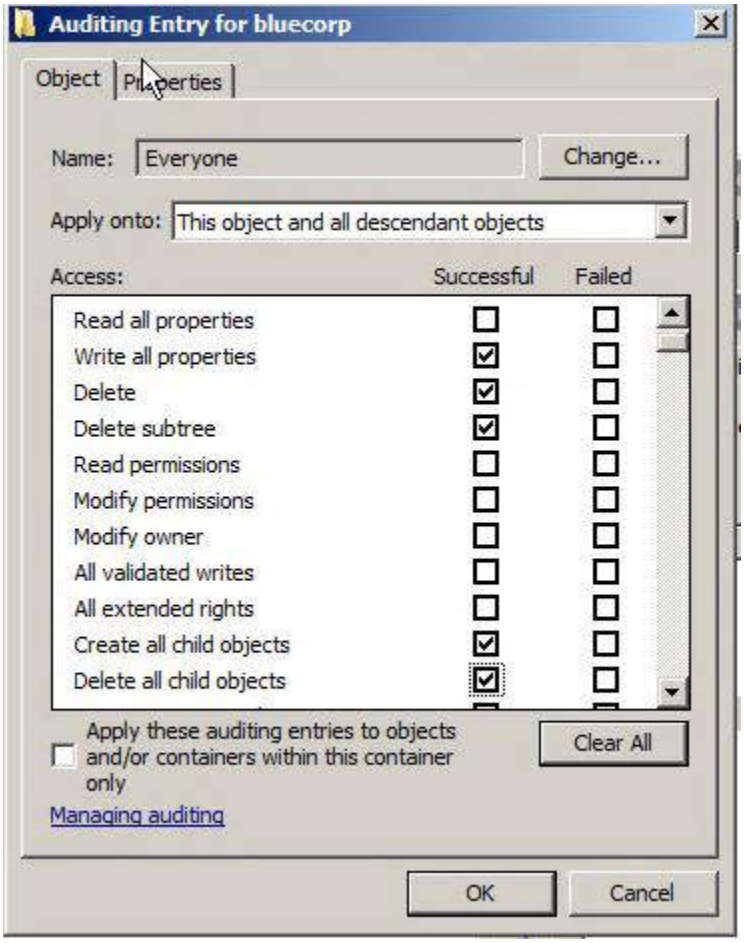


5. Click Add to create a new audit entry and select the object Everyone.as shown below

Note: You can also modify an existing audit entry instead of adding a new one.

6. Check the following access rights:
    a. Write all properties
    b. Delete
    c. Delete subtree
    d. Create all child objects
    e. Delete all child objects

(Note: All create and delete entries will get checked automatically)



7. Click Ok to save setting.

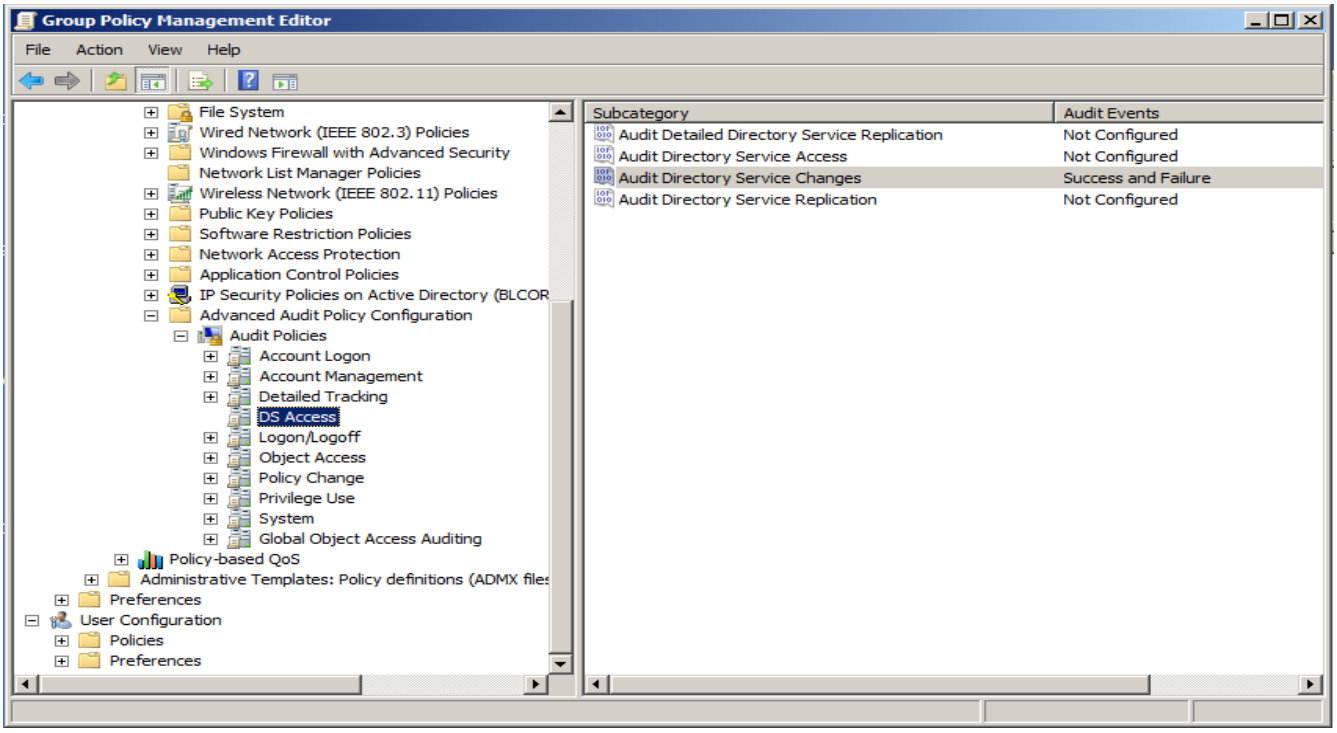
NOTE: If your Active Directory environment contains multiple OU's that do not inherit from the parent domain object, you may need to create similar audit entries for those OU objects.

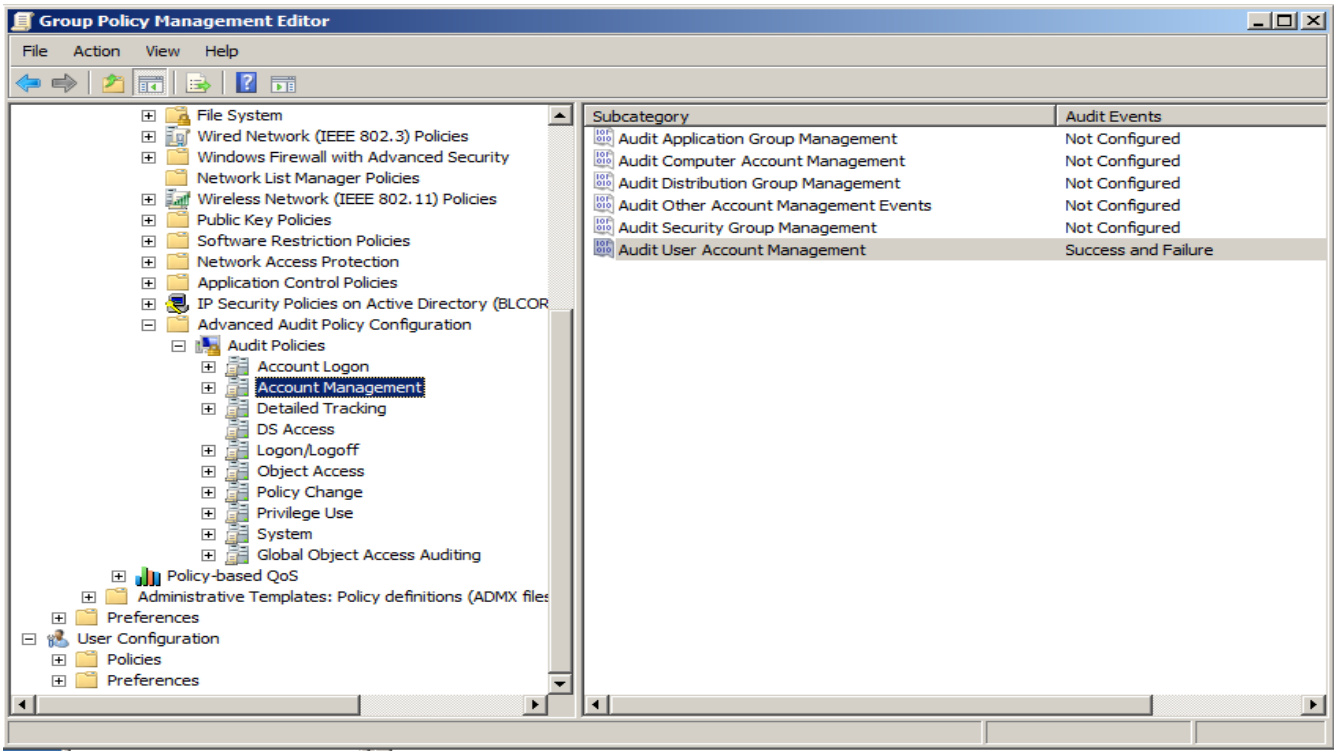
Advanced Auditing Polices for the Default Domain Controller Group Policy

The second step requires audit entries to be defined on the default group policy for Domain Controllers. Use the Group Policy Management MMC to access Advanced Audit Polices and configure the following audit entries

Audit Policy	Sub Category	Audit Events
DS Access	Audit Directory Service Changes	Success and Failure
Account Management	Audit User Account Management	Success and Failure
Object Access	Audit SAM	Success and Failure

Example of a Default Domain Controller GPO configured to audit Active Directory events for LT Auditor+.



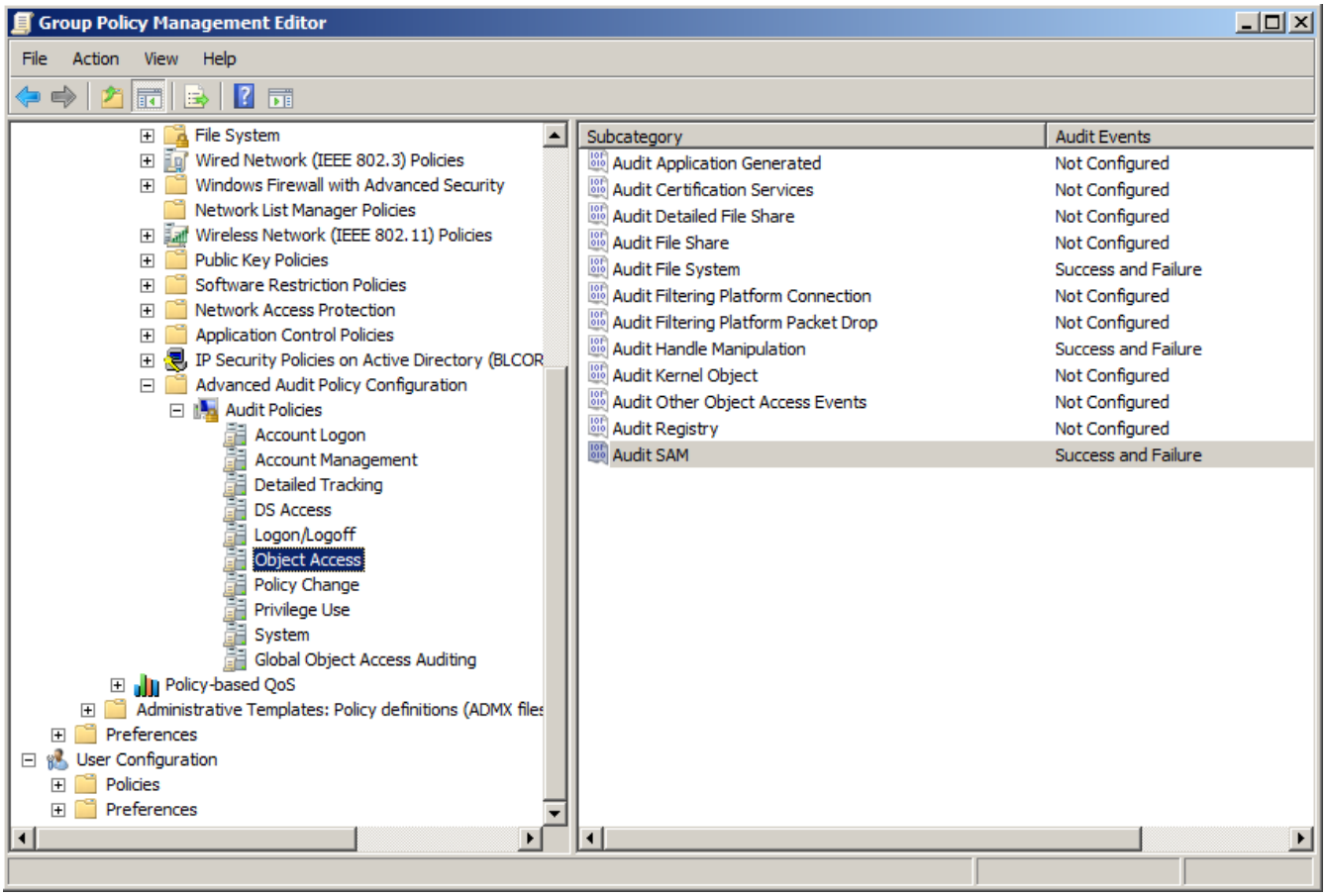


FILE SYSTEM

To audit files and folder, the following audit entries need to be configured on the GPO associated with the OU that contains the file servers.

Audit Policy	Sub Category	Audit Events
Object Access	Audit File System	Success and Failure
Object Access	Audit Handle Manipulation	Success and Failure

Example of Default Domain Controller GPO configured to audit File System activity for LT Auditor+.



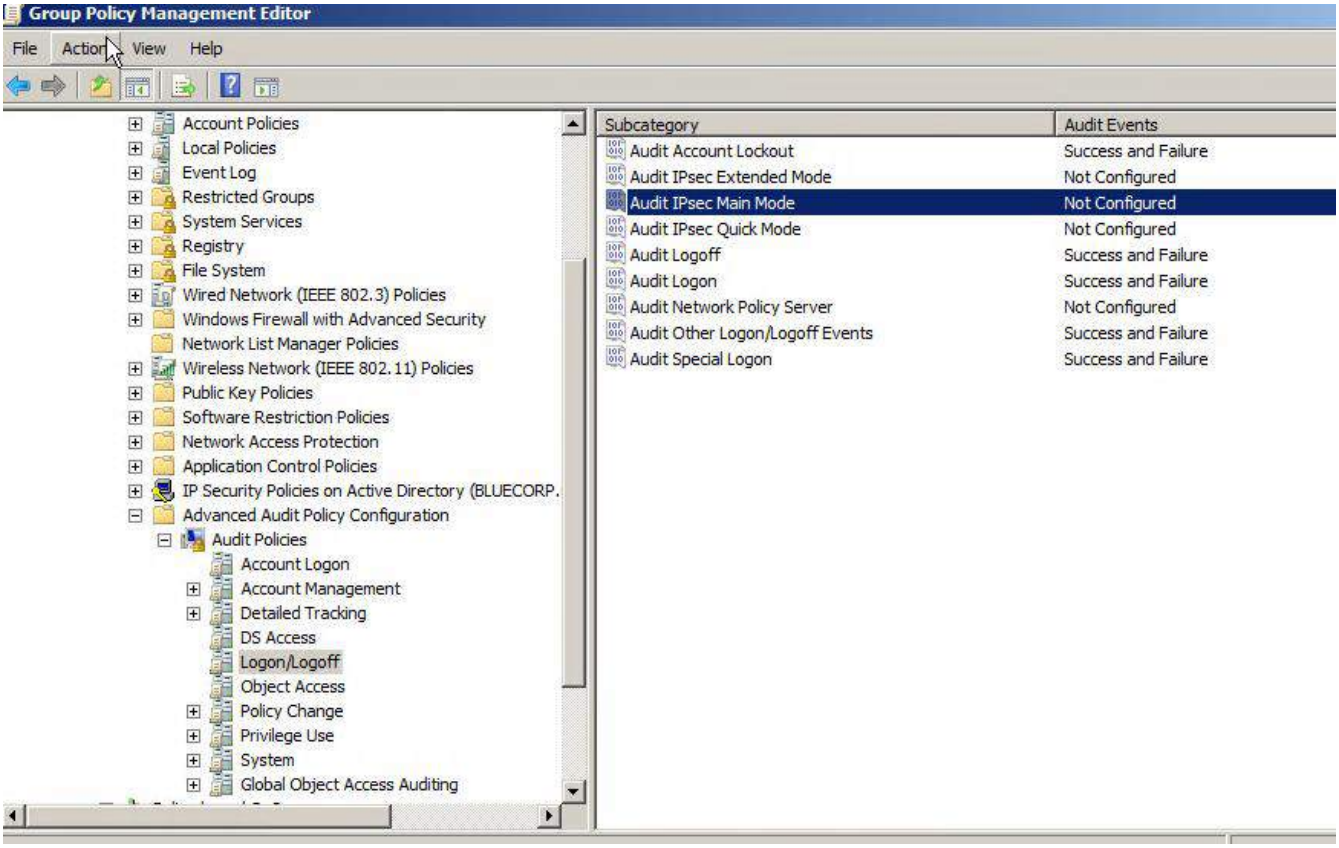
LOGIN/LOGOUT

To audit login and logout activity on Windows, the following audit entries need to be configured on the GPO associated with the OU that contains the servers. Blue Lance recommends that these setting are defined for the Default Domain Group Policy

Audit Policy	Sub Category	Audit Events
Account Logon	Audit Kerberos Authentication Service	Success and Failure
Login/Logoff	Audit Account Lockout	Success and Failure
Login/Logoff	Audit Logoff	Success and Failure
Login/Logoff	Audit Logon	Success and Failure
Login/Logoff	Audit Other Logon/Logoff Events	Success and Failure

Login/Logoff	Audit Special Logon	Success and Failure

Example of Default Domain Controller GPO configured to Login/Logout activity:

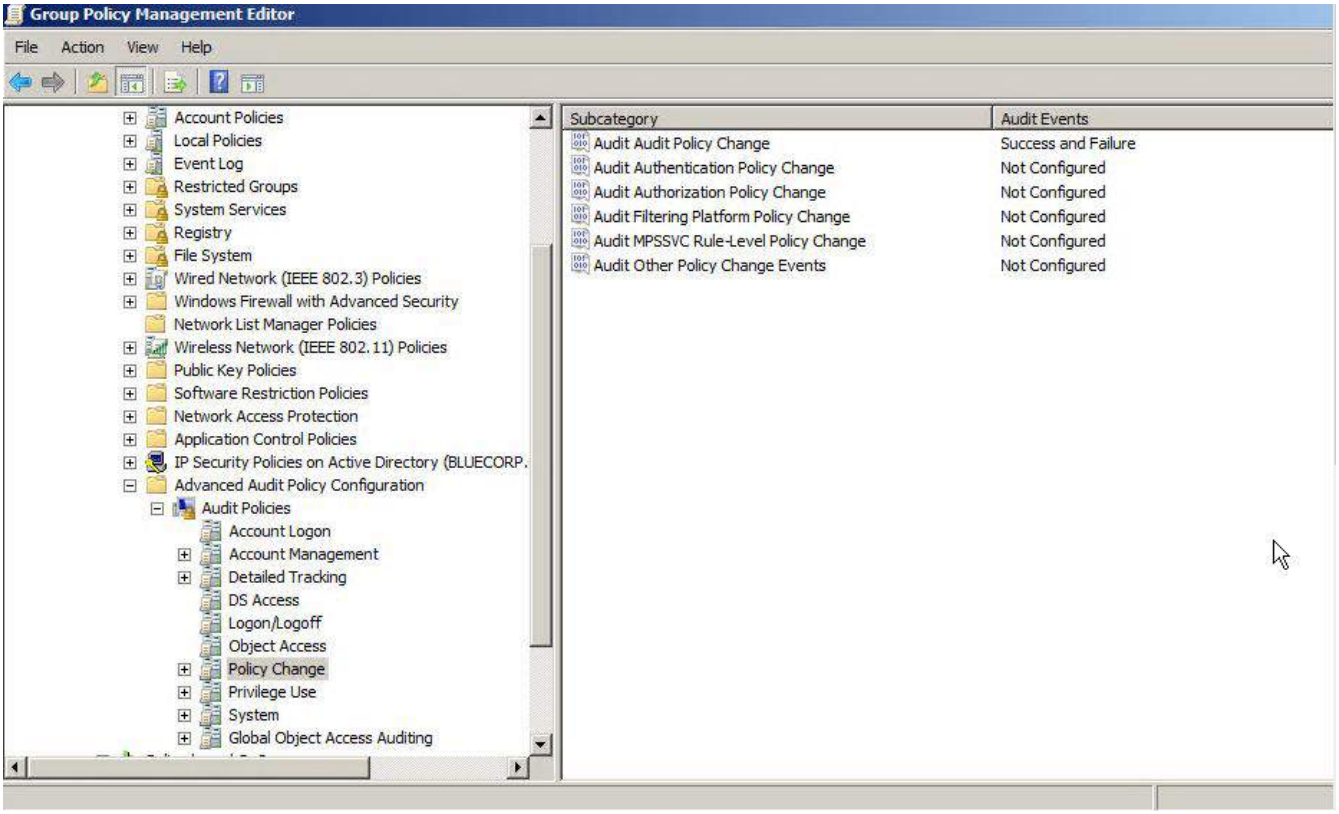


AUDIT POLICY CHANGES

To audit changes to audit policies the following audit entries are required:

Audit Policy	Sub Category	Audit Events
Policy Change	Audit Policy Change	Success and Failure

Example of Default Domain Controller GPO configured to audit policy changes:



APPENDIX A – WINDOWS EVENT ID's USED BY LT AUDITOR+

ACTIVE DIRECTORY

Category	LT Auditor+ Event	Object	Windows Event ID
Object			
	Create Object		5137
		User	
		Global Security Group	
		Domain Local Security Group	
		Computer	
		Domain Local Distribution Group	
		Global Distribution Group	
		Universal Distribution Group	
		Universal Security Group	
		Other	
	Delete Object		5141
		User	
		Global Security Group	
		Domain Local Security Group	
		Computer	
		Domain Local Distribution Group	
		Global Distribution Group	
		Universal Distribution Group	
		Universal Security Group	
		Other	
	Modify Security DACL		5136
	Rename Object		4781
	Move Object		5139
	Add Attribute		5136
	Delete Attribute		5136
Account Modification			
	Enable Account		4722
	Disable Account		4725
	Set Password		4724
	Change Password		4723
	Account Locked		4740

	Account Unlocked		4767
Group Membership			
	Add Member to group		5136
		Global Security Group	
		Domain Local Security Group	
		Domain Local Distribution Group	
		Global Distribution Group	
		Universal Distribution Group	
		Universal Security Group	
	Remove Member from group		5136
		Global Security Group	
		Domain Local Security Group	
		Domain Local Distribution Group	
		Global Distribution Group	
		Universal Distribution Group	
		Universal Security Group	
	Trusted domain added		4706
	Audit policy changed		4719

WINDOWS FILE SYSTEM

Category	LT Auditor+ Event	Windows Event ID
File		4656
	Create File	
	Write File	
	Rename File	
	Delete File	
	Access File	
Directory		4656
	Make Directory	
	Remove Directory	
	Rename Directory	
	Access Directory	
File Directory		4656
	Write Security DACL	

	Write Attribute	
	Take Ownership	