**Step 1: Enabling the Security Auditing**

For security auditing, it is required to modify the existing default Domain’s policy, which is setup while creating a domain. You have to, in fact, deal with Advanced Audit Policy Configuration for this. Follow the steps below for enabling the security auditing of Active Directory in Windows 2008 R2.

1) Go to “Start Menu” ►“Administrative Tools” ►“Group Policy Management”   
2) In the console tree in the left pane, go to “Forest” ►“Domains” ►Domain Name. Expand it   
3) Right click on “Default Domain Policy” and click “Edit”. It will show “Group Policy Management Editor”   
4) Go to “Computer Configuration” ►“Windows Settings” ►“Security Settings” ►“Advanced Audit Policy Configuration” ►“Audit Policies”. This will list all available audit policies   
5) Here, you can enable the following policies for following purposes :

(I) Domain Logon/Logoff Auditing   
In “Logon/Logoff”, enable :   
(a) Audit Logon   
(b) Audit Logoff

(II) File System Auditing   
In “Object Access”, enable :   
(a) Audit Detailed File Share   
(b) Audit File Share   
(c) Audit File System

(III) Handle Manipulation Auditing   
In “Object Access”, enable :   
(a) Audit Handle Manipulation

6) Double-click any of the events listed in the above table to access its properties   
7) Check the box “Configure the following audit events” and then enable the required “Success” and “Failure” events   
8) Click “Apply” and “OK” to enable the monitoring for the selected events

Similarly, you can configure the advanced auditing policies for other available options as well.

## Step 2: Enabling the Global Object Access Auditing

Perform the below mentioned steps to audit the access of any object globally in the server :

1) Go to “Start Menu” ►“Administrative Tools” ►“Group Policy Management”   
2) In the console tree in the left pane, go to “Forest” ►“Domains” ►Domain Name   
3) Right click on “Default Domain Policy” and click “Edit”. It will show “Group Policy Management Editor”   
4) Go to “Computer Configuration” ►“Windows Settings” ►“Security Settings” ►“Advanced Audit Policy Configuration” ►“Audit Policies”   
5) Go to “Object Access”. This will show the audit policies of object access in the right panel   
6) Double-click “Audit Registry” to show its properties box   
7) Check the box “Configure the following audit events” and check the both events   
8) Click “Apply” and “OK”   
9) Now, go to “Global Object Access Auditing” node under “Audit Policies” of   
advanced configuration   
10) Double-click “Registry” entry in the right details pane   
11) Check the box “Define this policy”. This will enable the subsequent button   
12) Click “Configure” to access the “Advanced Settings for Global Registry SACL”   
13) Click the “Add” button to add the users which access you want to audit   
14) Type the name of any user to be audited   
15) Click “Check Names” to validate them   
16) Click “OK” for adding the users. This will show the auditing entries for that user   
17)Select the audit entries for both success and failure, which you want to   
monitor and click the “OK” button. It is advised to select Full Control for both   
of them   
18) Click “OK” once the required entries are selected. This will take you back to the “Advanced Security Settings”   
19) You can follow the same steps to configure security auditing for other users   
20) Once done, click “Apply” and “OK”. You will be returned to “Registry   
Properties”   
21) Click “Apply” and “OK” once again

Thus, you can follow the above mentioned steps to configure the advanced file system auditing by using the “File System” policy in “Global Object Access Auditing”

## Step 3: Managing the Integrity of Advanced Auditing

The advanced auditing entries are often overwritten by that of basic auditing.

Follow the steps below to ensure that the advanced auditing entries do not get overwritten :

1) Go to “Start Menu” ►“Administrative Tools” ►“Group Policy Management”   
2) In the console tree left pane, go to “Forest” ►“Domains” ►Domain Name   
3) Right-click on “Default Domain Policy” and click “Edit”. It will show “Group Policy Management Editor”   
4) In the left tree pane, go to “Computer Configuration” ►“Policies” ►“Windows Settings” ►“Security Settings” ►“Security Options”   
5) Double-click “Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings”   
6) Click “Define this policy setting” and click “Enabled”   
7) Click “Apply” and “OK” to close the dialog box

This will apply the modified security auditing policies on the server. Alternatively, you can logoff and logon the Administrator. It is required to update the modified Group Policies on the server after enabling the security auditing policies.

## Step 4: Verifying the Auditing Policies

It is recommended to verify whether the modified auditing policies have been applied or not. Run the following command on the Command Prompt :   
auditpol.exe /get /category:\*

This will list the status of all auditing policies– both basic and advanced on the server.   
Please verify both “Success” and “Failure” events for the policies, which you have enabled.