Audit account logon events

Description

This security setting determines whether to audit each instance of a user logging on to or logging off from another computer in which this computer is used to validate the account. Account logon events are generated when a domain user account is authenticated on a domain controller. The event is logged in the domain controller's security log.

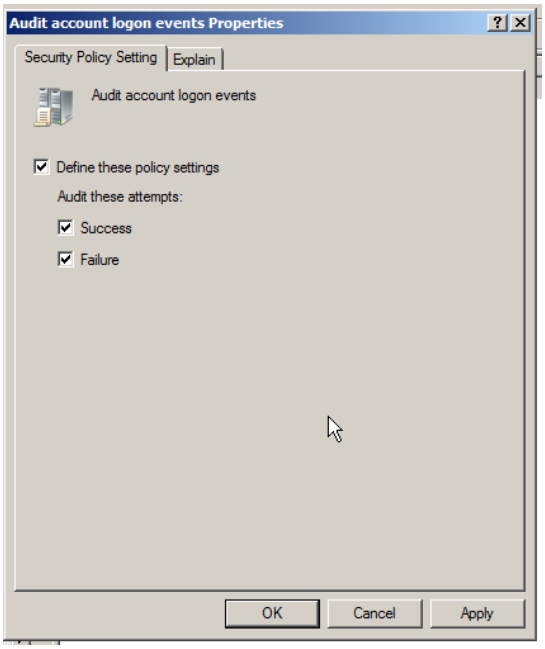
If success or failure auditing for account logon events is enabled on a domain controller, an entry is logged for each user who successfully or unsuccessfully validates, even though the user is actually logging on to a client that is joined to the domain.

If you define this policy setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when an account logon attempt succeeds. Failure audits generate an audit entry when an account logon attempt fails.

Configuring this security setting

To configure this security setting for the domain controllers in the domain:

Open **Group Policy Management** and browse to the **Default Domain Controller Policy** object. Right-click, on the object and select edit. Expand the console tree as such: **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit Account Logon Events**. View the properties of this item and configure as desired:



To set this value to track login **Successes**, select the **Define these policy settings** check box and check off the **Success** check box.

To set this value to track login **Failures**, select the **Define these policy settings** check box and check off the **Failure** check box.

Select both if you wish to track both.

To set this value to **No auditing**, select the **Define these policy settings** check box and clear the **Success** and **Failure** check boxes.

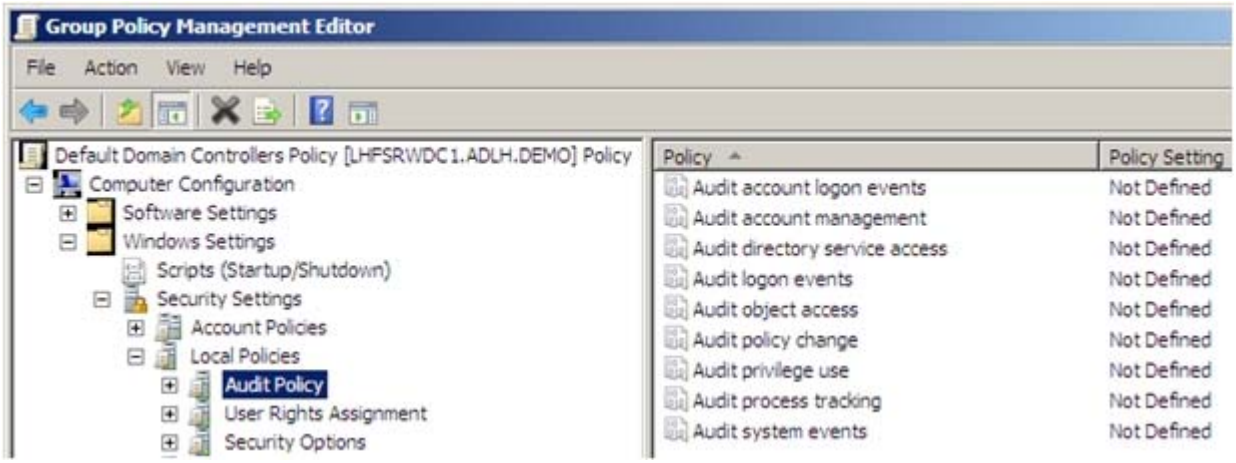
To ensure the policy is immediately implemented, execute the **GPUPDATE** command at a command prompt on the server.

Events are logged to the **Windows Security log** and can be viewed within **Event Viewer**. Each logged entry includes an Evident ID# and, if it's a failed login, a Failure Code. This is useful information; an administrator might choose to simply track occurrences of events (i.e, account lockouts) or could use these entries for troubleshooting purposes. The ultimate windows security website is a good resource to learn more about event IDs.

Changes between Windows 2000/2003 and Windows 2008

Looking inside the "Default Domain Controllers" GPO of a 2000/2003 AD domain you will see the following default settings for the main event categories

Looking inside the "Default Domain Controllers" GPO of a 2008 AD domain you will see the following default settings for the main event categories

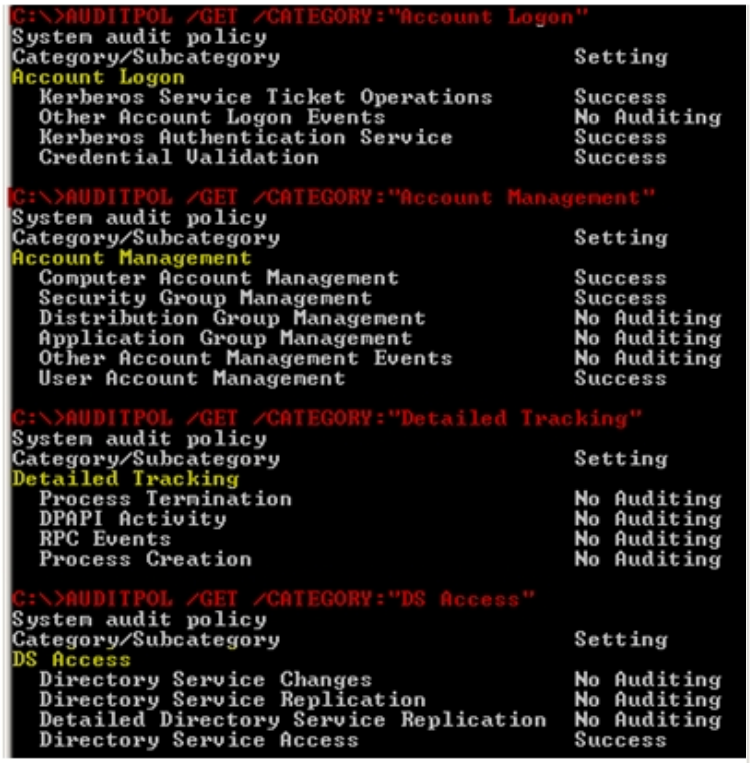


It looks as if the Windows 2008 default account policy values have been changed; however, this isn't the case. Microsoft has broken the main event categories into sub event categories (aka Granular Audit Policies (GAPs)) and has configured the same default values as were configured in previous versions of Windows however have set these values within sub event categories. There are about 50 sub event categories. You can manage auditing either at the main category level (the original nine policies) or at the subcategory level.

When a main event category is configured with a value within the GPO, all of the sub event categories are also configured with the same value. For example, if you set the Audit Account Logon Events

policy to track successful logons as well as failed logons, all sub categories will be configured to track both. Since the sub categories are not visible within GPO, you might ask: "How do I configure the sub event categories through a GPO?" The answer is easy. You just don't. Sub event categories can only be configured through the AUDITPOL.EXE command.

The picture below displays the commands to view the settings of both main and sub event categories on a Windows Server 2008 server. The yellow text is the main event category that corresponds with the main event category in the GPO(s). The white text below that are the sub event categories of each main event category. (You can also view all categories (main and sub) with the following command: auditpol /get /category:*)



Using AUDITPOL to view and set Sub Event Categories

To view the command's syntax and all available parameters:
auditpol /?

To view the current settings for *all* main event categories and their respective sub event categories:
auditpol /get /category:*

Word of caution on this one:
If you use /set instead of /get in the above command you will enable success on ALL subcategories. It might be a good idea, before 'playing' with some of these commands, to store the current default settings for each of the subcategories in a text file (auditpol /get /category:* > defaultvals.txt). Should you reset all by mistake you at least will have access to the default values in the text file and you could then manually reset each.

To view a list of all the main category names:
auditpol /list /category

To view the current settings for a specific main event category and its sub event categories:
Auditpol /get /category:"*main event category name"*
Example: auditpol /get /category:"Account Logon"

To set a sub event category:
Auditpol /set /subcategory:"*Sub event category name"* /success:*value* /failure:*value*
Example:
auditpol /set /subcategory:"Kerberos Authentication Service" /success:enable /failure:disable

Two important things to note about using subcategories:

- Subcategories are not part of the Group Policy Object therefore they are not 'pushed' to other computers. Policies set with auditpol are set locally on that machine. The policies covered in this document are policies that would typically be configured on a domain controller. If you have more than one domain controller in your domain you would most likely want these policies 'pushed' to all other domain controllers in the domain.

  One way to resolve this is to create a batch file which contains auditpol commands that set the subcategories to the desired settings and then configure the batch file to execute at each domain controller when it starts. *This* can be configured using Group Policy Management: edit the Default Domain Controller Policy object: **Computer Configuration\Policies\Windows Settings\Scripts\Start Up.** Click on **Show Files**, store the batch file in this *startup* folder and close Windows Explorer. Click on the **Add** button and add the batch file to the Startup policy.

- Audit settings configured using a Group Policy Object take precedence over audit settings configured locally. So…. If you use the auditpol command (either on one server or through scripts on many servers) and then you (or someone else) enables policies within the Default Domain Controller GPO, the GPO settings will overwrite the local settings established with the auditpol command.

To avoid this from happening you can configure a policy to force the subcategories configured through auditpol to have precedence over policies set with a GPO. *This* can be configured using Group Policy Management: edit the Default Domain Controller Policy object: **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options. Enable *Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings.***