

Auditing ?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-05/0312.html>

From: Drumgod (Drumgod_at_discussions.microsoft.com)

Date: 05/24/05

Date: Tue, 24 May 2005 07:40:01 -0700

All,

I am configuring an audit policy for my network. Security is pretty tight here and they are requiring me to audit the entire C: drive for object access. I am currently auditing the user group 'Authenticated Users' for Success/Failure on the following:

Create Files / Write Data
Create Folders / Append Data
Delete

Now this works as expected, but its also producing object access events with the username of 'System'.

I do NOT want to audit system events. Is the system part of the authenticated users group, and if so , what group should i be auditing (on my domain).

I have disable the GPO object to audit system events. Computer Configurations | Windows Settings | Security Settings | Local Policies | Audit Policy | Audit System Events is set to "No Auditing". I am doing this a the domain root and im only a single domain. No connection to any other domains at all. But im still getting events for object access by the 'system' account. This is obviously filling up my security logs rather quickly, and I dont care what the system is doing.

Anyone know what im doing wrong on this ? How do i get rid of the object access from the system?

TIA

Drum on