

Re: Auditing.. We all love it...

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.group_policy/2005-04/msg00497.html

- *From:* "Ryan Hanisco" <rhanisco@xxxxxxxxxxxxxxxx>
 - *Date:* Fri, 29 Apr 2005 16:16:26 -0500
-

Remember that the system is a security principal too and a consumer of system resources, thus creating events. You can filter events so you don't see them. This might be the best way to get what you want.

--
Ryan Hanisco
MCSE, MCDBA
FlagShip Integration Services
Chicago, IL

"Drumgod" <Drumgod@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:DF18B7ED-1663-4A30-A312-818EFB6F55E3@xxxxxxxxxxxxxxxx

> All,
>
> I am working at a government site. The security here is really high. I
> have
> to enable auditing for the entire %SystemDrive% on each workstation.
> That's
> the easy part.
>
> I have the auditing configured using a GPO Computer Configurations |
> Windows
> Settings | Security Settings | File System. I have setup a standard set of
> NTFS permissions, and I have applied auditing to the entire drive using
> this
> GPO. Now, when I view my security log file I have WAY TOO MANY 'SYSTEMS'
> audits for object access. Now, object access is what Im trying to audit
> for
> all users, but not for the system. Im mean, who really cares what the
> system
> is doing...
>
> So my question is , how to I audit object access for all users and omit
> the
> system activities from being audited. ???
>
> I have auditing setup to audit anyone in the authenticated users group. If
> I

Re: Auditing.. We all love it...

- > change this to say, domain users, will the system object access events
- > leave
- > my securiry log?????
- >
- > Any ideas??? (BTW, Auditing SUCKS!)
- >
- > Drum on

• **References:**

- ◆ **Auditing.. We all love it...**
 - ◇ *From:* Drumgod
- Prev by Date: **Re: Reset password**
- Next by Date: **Re: terminal server config**
- Previous by thread: **Re: Auditing.. We all love it...**
- Next by thread: **Reset password**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**