

# Re: Audit Policy

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2006-06/msg00018.html>

---

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
  - *Date:* Mon, 5 Jun 2006 08:57:43 -0700
- 

First, your maximum log size is too large. With W2k3 and prior there is a hard limit on the usable quantity of a specific heap in the system, which is shared for a number of purposes. The current Microsoft recommendation is the the sum of all event logs be no more than something in the 300 to 400 meg range.

That said, you have too much enabled for logging if you are having a gig roll off within the day, or you have a very large environment perhaps with too few DCs.

Object access is for such as NTFS auditing and only cuts a record if enabled and access is made to an object where an audit SACL has been set for the type and origin of the access.

Privilege Use triggers a record when a user token is loaded with user privilege flags that are "above" the normal.

Try getting the security and hardening guides which explain audit settings and suggests what may work for different environments.

What you need depends on many things, including your compliance constraints, corp policy, etc.. Keep in mind that there is an impact from excessive event logging.

"George Schneider" <georgedschneider@xxxxxxxxxxxxxxxx> wrote in message <news:BC583F47-3072-4C4E-B35F-B2B2E3EF6299@xxxxxxxxxxxxxxxx>

I was taking a look at my event logs and noticed that the security log contains tons of 576 and 578 events for Priviledge Use. In our group policy

I have it set to overwrite events a sneeded which presents a problem with some

many events being logged. The maxium log size is set to 1024 kb. Events overwritwe each other before the end of a day. What is Priviledge Use? My thought is that I should change our Audit policy to audit only failures.

I went into Group Policy and changed the audit settings for Audit object access

to falure instead of success, failure. I thought this would fix the problem. What audit policy setting will determine success, failure audit for

priveldge use.

Re: Audit Policy