

Re: GPO causing client security logs to fill?

that are
logged
into from other computers. Specifically, one of them has a
printer
attached
and the other is a server for our accounting program.

The event ID's are as follows 515, 528, 538, 540, 552, 576,
680, 858

When I view the event logs through server management the
properties for
the
security event log indicate that it is to overwrite messages
older than
7
days. In one case the log is full with only two days worth of
events.
Of
course this is the PC that is the accounting server.

I assume that this is as a result of a GPO change. I also
assume that
with
the change either the log clearing properties were
unknowingly changed
or
a
change was made with regard to what is recorded in the log.
Unfortunately,
I
don't really know what items to look at or which ones are
safe to
change.

All event logs should be set to a decent size (about 20MB at minimum,
more
on the server esp for app/system), and set for "overwrite as needed".

This can be controlled via GPO –

computer config\windows settings\security settings\event log

...but I'd run an rsop.msc on one of the problem computers to see what's
been set, and from where.

Re: GPO causing client security logs to fill?