

Re: Print Auditing

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2004-04/0075.html>

From: Derek Melber [MVP] (derekm_at_braincore.net)

Date: 04/09/04

Date: Fri, 9 Apr 2004 13:57:49 -0700

Adrian... WOW, that is another issue, and yeah, he is bold. How about this:

- 1) Setup auditing on the Print Queue itself.
- 2) Only configure successful writes to the queue, not failures.
- 3) This should not require any new auditing from the domain level, what you have configured should be fine.

This is not perfect, but it will tell you which files were written to the queue. If they are named Page1.bmp or something, it won't help much... but you will get the "perp" or "perv" (which ever you want to use:--) in the audit trail.

--

Derek Melber
BrainCore.Net

derekm@braincore.net

"Adrian Moseley" <amosley@personix.fiserv.com> wrote in message
news:Oi9e8GnHEHA.2376@TK2MSFTNGP12.phx.gbl...

>

> I've followed the suggestion, but this is the type of information I
receive:

>

> Event Type: Success Audit
> Event Source: Security
> Event Category: Object Access
> Event ID: 560
> Date: 4/6/2004
> Time: 3:52:52 PM
> User: STAFFORD\amosley
> Computer: PXHOUWADM
> Description:
> Object Open:
> Object Server: Spooler
> Object Type: Printer
> Object Name: HP Business Inkjet 2230/2280
> New Handle ID: 13232176
> Operation ID: {-,-}
> Process ID: 2276
> Primary User Name: PXHOUWADM\$
> Primary Domain: STAFFORD
> Primary Logon ID: (0x0,0x3E7)
> Client User Name: amoseley
> Client Domain: STAFFORD
> Client Logon ID: (0x0,0xB4B7)

microsoft.public.windows.server.security: Re: Print Auditing

```
> Accesses Print
>
> Privileges -
>
>
> This is great, but Is there a way to get a log of the actual files that
were
> printed?? We are trying to catch someone who is printing out PORN to our
> color printer... This guy is BOLD!! Thanks in advance.
>
>
> "Derek Melber [MVP]" <derekm@braincore.net> wrote in message
> news:urtBLgmHEHA.2556@TK2MSFTNGP12.phx.gbl...
> > configure auditing for objects, a printer is an object, like folders,
> files,
> > registry keys, and AD objects.
> >
> > --
> > Derek Melber
> > BrainCore.Net
> > derekm@braincore.net
> > "Adrian Moseley" <amoseley@personix.fiserv.com> wrote in message
> > news:ui0P40mHEHA.1048@TK2MSFTNGP12.phx.gbl...
> > > My managers would like to have auditing for printing so we can see a
> list
> > of
> > > who prints what. I have looked through the windows KB and found a
> document
> > > to help me start this procedure but it seems a bit imcomplete.
> > >
> > > KB document:
> > >
> > >
> > >
> > > http://support.microsoft.com/default.aspx?scid=kb;en-us;323228&Product=win2000
> > > States "How to track Printer Usage"
> > >
> > > When I go to Security/Advanced/Auditing and choose a user to audit, I
> get
> > > the following message:
> > > "The current Audit Policy for this computer does not have auditing
> turned
> > > on. If this computer gets audit policy from the domain, please ask a
> > domain
> > > administrator to turn on auditing using Group Policy Editor.
Otherwise,
> > use
> > > the Local Computer Policy Editor to configure the Audit policy locally
> on
> > > the this computer."
> > >
> > > We are still using an NT 4.0 Domain, so I configuring through local
> > policy.
> > > But I do not know with object to audit that will only tell me who
> printed
> > a
> > > document and what the document was....
> > >
> > > I believe i have seen this on NT 4.0, where do I go to set this up
for
> > > 2000? Thanks.
> > >
> > >
```

microsoft.public.windows.server.security: Re: Print Auditing

> > >
> >
> >
>
>