

Re: trace user logons

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2003-10/0149.html>

From: Peter (*parvo_at_REMOVETHISrtc-employment.com*)

Date: 10/17/03

Date: Fri, 17 Oct 2003 09:19:11 -0400

Check to see what the "Effective Setting" is under the "Audit Policy" on one of your servers or workstations. If it doesn't say "Success, Failure", then a setting is either not correct on the Domain Controller or the policy is not being distributed. This is my best guess...

"John" <organic_john@yahoo.com> wrote in message
news:OU87Q7IIDHA.1884@TK2MSFTNGP09.phx.gbl...

> *thanks for replies folks.....*

> *Yeah, i had several of the local audit policies enabled under Domain*

> *Security Policy, but still the security log was empty. I've enabled all of*

> *the local audit policies now, but still nothing is appearing in the*
security

> *log. I've checked the filter on the security log, and it is set to show*

> *between the first and last event.*

>

> *I've gone into Domain Controller Security Policy aswell, and ensured some*

> *auditing was on there. Again, nothing is appearing in the security logs.*

>

> *any other suggestions?*

>

> *thanks again*

> *j*

>

> *www.banwa.com*

> *"Peter" <parvo@REMOVETHISrtc-employment.com> wrote in message*

> *news:Ox8JUe\$kdHA.744@tk2msftngp13.phx.gbl...*

> > *Keith is correct. I would highly turn on auditing domain wide, by doing*

> *the*

> > *following from your Win2000 Domain Controller(if you are using something*

> > *other than Windows 2000 the procedure will be different).*

> >

> > *Goto Start>Programs>Administrative Tools>Domain Security Policy*

> >

> > *Open Security Settings>Local Policy>Audit Policy*

> >

> > *Go into each of the policies you want to enable by double clicking on*
them

> > *in the right pane, and check the appropriate boxes. I have them all*

> *enabled*
> > *on my server.*
> >
> > *Hope this helps...*
> >
> > *"Keith W. McCammon" <km@km.com> wrote in message*
> > *news:%23wY2RP\$kDHA.2216@TK2MSFTNGP12.phx.gbl...*
> > > *You need to enable auditing on your DC's, which will populate all*
> *manner*
> > *of*
> > > *information in the security event logs. Information and how-to's on*
> > > *auditing can be found on TechNet, or in your help file.*
> > >
> > >
> > > *"John" <organic_john@yahoo.com> wrote in message*
> > > *news:e1J2MI\$kDHA.2200@TK2MSFTNGP12.phx.gbl...*
> > > > *thanks in advance for any assistance:*
> > > >
> > > > *I'm trying to find out when someone has logged onto our network, i*
> > > > *presumed*
> > > > *it would have shown under the even viewer and security log of the*
> *Domain*
> > > > *Controller, but it is empty.*
> > > >
> > > > *Is this the correct place to view such info as successful logons or*
> > > > *unseccuessful logons? If so, any suggestions as to why they are not*
> > > > *showing.*
> > > >
> > > > *If this is not the correct place to view this data, where should i*
> *be*
> > > > *looking.*
> > > >
> > > > *regards*
> > > > *john*
> > > >
> > > >
> > > >
> > > >
> > >
> > >
> >
> >
> >
>
>