

Re: Question About Auditing

Source:

<http://www.tech-archive.net/Archive/Certification/microsoft.public.cert.exam.mcse/2004-03/3588.html>

From: TechGeekPro (%username%_at_yahoo.com)

Date: 03/22/04

Date: Mon, 22 Mar 2004 17:54:19 -0500

Why on earth would I want to Google it myself!? Isn't that what this newsgroup for!?

(wink, wink, hint, hint, clue, clue) And btw, that's "TechGeek'Pro" to you Neil. <big grin>

Seriously, thanks for all the help (especially for the obligatory TinyUrl), it helped clear things up.

One other point of interest:

I notice there were no replies from the "so called" MCNGP's. I guess the majority of them were too busy feeding their massive egos by being a**h***'s to those less "experienced" than them.

Tis' a Shame.

--

There are 10 types of people in the world:
Those who understand binary, and those who don't...
"Neil" <neilmcse@nospamforyou.com> wrote in message
news:Xns94B4652FA1FFDneilmcsehotmailcom@207.46.248.16...
> "Julian Ford" <julian_ford@btopenworld.com> wrote in
> news:#nyqKh#DEHA.1228@TK2MSFTNGP11.phx.gbl:
>
> > My understanding of this is that if you access a resource (file etc.),
> > on a file server for example, it is a loggon event, if you access a
> > resource on a DC it is an Account Loggon event. Conversely, if you
> > log onto the network from a server or workstation it is a loggon, if
> > you log at a DC it is a Account logon.
> >
> + Rowdy says:
> >> sort of. you authenticate with a DC, so if you audit account logon's
> >> at
> > the
> >> DC's, you will track when which user has logged on in AD (i.e. your
> >> network).
> >>
> >> if you audit just logon events at the workstatain level, you can track
> >> when who has authenticaed on the local machine.
> >>
>
>
> here it is from the horse's mouth (amazing what googling will do...nudge,
> nudge, wink, wink, get a browser <grin>
>
> <http://www.microsoft.com/technet/prodtechnolog/windows2000serv/maintain/mon>

microsoft.public.cert.exam.mcse: Re: Question About Auditing

```
> itor/logevnts.mspx
>
> and the obligatory
>
> http://tinyurl.com/2sbyk
>
> TechGeek, both Rowdy and Julian have part. Logon is for access to
> resorces that require logon to a machine not the Domain. Account Logon is
> Domain Authentication. When you access a member server or workstation for
> a resource you need to be validated by that servers using a local logon
> event and the logon event is tagged in the security logs. the first 2
> paragraphs in the article pretty much explain the whole dodad...
>
> HTH
>
> --
> Neil
> "you'd do what, to who, for how many biscuits?"
```