

Re: DC Policy: just want to audit files, not set security

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-03/0313.html>

From: Roger Abell (*mvpNOSpam_at_asu.edu*)

Date: 03/17/05

Date: Thu, 17 Mar 2005 11:12:22 -0700

"Steven L Umbach" <n9rou@nospam-comcast.net> wrote in message news:uxyD1txKFHA.656@TK2MSFTNGP14.phx.gbl...

> *You are right Roger. I did not pick up on that part. Too bad file system*
> *permissions work that way where you can not use it to just enable*
> *uditing. --- Steve*
>

Yes, it is too bad. I had never considered the case before. For this person, the particular directory to root the auditing makes it perhaps the most difficult case since there are so very many subdirectories and individual files with explicitly set, different permissions within the area. This makes setting a DACL for the root of the area to be audited very complex. I did not test, but if I recall, one can exempt subareas by naming them in the template, setting them to not be changed; the question then is, will the SACL for auditing still propagate into those areas? Another test.

--

Roger

>
> "Roger Abell" <mvpNOSpam@asu.edu> wrote in message
> news:eHvKdkrKFHA.1172@TK2MSFTNGP12.phx.gbl...
> > You may a slightly misread the poster.
> >
> > I had never thought of using a SCE template File System
> > definition to deliver only Audit SACL to some storage
> > area, but I immediately thought I saw what the poster
> > was indicating. Hence, I tried it out, and in fact if the
> > DACL part is left empty with only a SACL definition
> > provided, then upon application the DACL on the target
> > storage is changed. That is, any explicit ACEs set on
> > the target are removed, and inheritance will be adjusted
> > (or not) depending on the settings choosen in the template.
> >
> > --
> > Roger
> > "Steven L Umbach" <n9rou@nospam-comcast.net> wrote in message
> > news:%23xDuJYpKFHA.2852@TK2MSFTNGP14.phx.gbl...
> >> They are separate. Be sure to limit auditing to just what is needed [

microsoft.public.windows.server.security: Re: DC Policy: just want to audit files, not set security

> >> write/delete maybe] as the security log will fill up very quickly if
you
> > try
> >> to audit everything. Just enabling auditing of object access will
> >> generate
> > a
> >> lot of events in the security log. Be sure to increase the size of the
> >> security log quite a bit to at least 20 MB to start. --- Steve
> >>
> >> <http://support.microsoft.com/default.aspx?scid=kb;en-us;301640> --- how
> >> to
> >> configure auditing.
> >>
> >>
> >> <-> wrote in message news:uv4XrRmKFHA.3500@TK2MSFTNGP14.phx.gbl...
> >> > Hello,
> >> >
> >> > I am being tasked with setting up auditing on the Windows directory
of
> > the
> >> > domain controllers via the Domain Controller Security Policy. They
> > don't
> >> > want to touch permissions on it. The thing is, the two seem linked
> >> > together. If I leave the security permissions blank, on the security
> >> > field and just go to auditing, and select a group and what to audit,
> > will
> >> > I run the risk of removing all permissions to the Windows directory?
> >> >
> >>
> >>
> >
> >
>
>
>