

Re: Audit Object Access

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2003-04/0944.html>

From: Steven L Umbach (n9rou@attbi.com)

Date: 04/14/03

From: "Steven L Umbach" <n9rou@attbi.com>

Date: Mon, 14 Apr 2003 21:57:39 GMT

Hi Selena. From what I read recently just enabling auditing of object access can generate a lot of entries because W2K will do auto auditing of what is called "base system objects". You can check your local security policy for the effective setting under security options for "audit the access of global system objects". If it is enabled or not defined try to disable it at proper security level and see if that helps reduce amount of entries. Also remember you can create a filter view in event viewer to make it easier to find particular entries. Also in event 560 check object name/type entries (file in particular) to double check if any auditing is enabled that you might not know about. — Steve

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/561.asp>

"Celina" <it@permasteelisa.com.hk> wrote in message
news:OBY1fJIADHA.2820@TK2MSFTNGP11.phx.gbl...

> Steve,

>

> *I only enable "Audit Object Access" in Local Security policy and run Secedit*

> *to refresh the policy. No file/folder is set to audit at the moment.*

> *However, once the policy enable. A lot of entries are generated. Here is the log entries details.*

>

> 1.

> *Event ID: 562*

> *User: Administrator*

> *Category: Object Access*

> *Description:*

> *Object Server: Security*

> *Handle ID: 180*

> *Process ID: 4264*

>

> 2.

> *Event ID: 562*

> *User: Administrator*

> *Category: Object Access*

> *Description:*
> *Object Server: Security*
> *Handle ID: 92*
> *Process ID: 4264*
>
> 3.
> *Event ID: 560*
> *User: Administrator*
> *Category: Object Access*
> *Description:*
> *Object Server: Security*
> *Object Type: Desktop*
> *Object Name: \Default*
> *Handle ID: 92*
> *Operation ID: {0,383179252}*
> *Process ID: 4264*
> ...
> *Accesses DELETE READ_CONTROL WRITE_DAC WRITE_OWNER Read Objects...*
>
> 4.
> *Event ID: 560*
> *User: Administrator*
> *Category: Object Access*
> *Description:*
> *Object Server: Security*
> *Object Type: WindowStation*
> *Object Name: \Windows\WindowStations\WinSta0*
> *Handle ID: 180*
> *Operation ID: {0,383179249}*
> *Process ID: 4264*
> ...
> *Accesses DELETE READ_CONTROL WRITE_DAC WRITE_OWNER Read Objects...*
>
> *Any idea?*
>
> *"Steven L Umbach" <n9rou@attbi.com> ¼¶¼g©ó¶l¥ó*
> *news:txqma.448109\$F1.65305@sccrnsc04...*
> > *File and folder auditing can generate a LOT of entries. I do*
some
> > *folder auditing , and a single event for one file can generate six or*
so
> > *entries because of all the system processes involved in*
> > *accessing/creating/deleting files. The best you can to is to try to*
audit
> > *an*
> > *absolute minimum of files and folders with and absolute minimum of*
entries
> > *in the access list. When setting audit permissions pay attention to the*
> > *"apply onto" drop down box. If you select files/folders/and subfolders*
> > *(which is default) on a folder you could potentially be auditing*
thousands

> > of files. --- Steve
> >
> > <http://www.jsifaq.com/SUBI/tip4000/rh4002.htm>
> >
> > "Celina" <it@permasteelisa.com.hk> wrote in message
> > news:#pp40JiADHA.1612@TK2MSFTNGP11.phx.gbl...
> > > Steve,
> > >
> > > I change the "Aduit Object Access" in domain controller security
policy
> > to
> > > "not defined" and in local policy to "Success". Then, select the
folder
> > > which I want to audit and in security policy, just select the "Delete"
> > > checkbox in "Success" colume. Run Secedit to refresh the policy. No
> > > action
> > > is done but the security log fill up a lot of entries with event id
560
> > &
> > > 562 and the user is administrator. However, the result is the same.
> > >
> > >
> > > "Steven L Umbach" <n9rou@attbi.com> ¼¶¼g©ó¶l¥ó
> > > news:eMLla.152627\$OV.236673@rwcrcsc54...
> > > > Sounds like you are auditing all file access and not just
> > > > deletions.
> > > > See link about ID descriptions. You need to fine tune what you want
to
> > > audit
> > > > on what files. If you want to audit just a specific domain
controller
> > > you
> > > > need to change domain controller policy to "not defined" for
auditing
> > > > object access so that it will not override local policy. -- Steve
> > > >
> > > > "Celina" <it@permasteelisa.com.hk> wrote in message
> > > > news:eG9skN\$\$CHA.2032@TK2MSFTNGP12.phx.gbl...
> > > > > I want to enable auditing files & folder deletion on a Win2k
server
> > > which
> > > > is
> > > > > also the domain controller. I try to enable object access in
Local
> > > > Security
> > > > > Policy but no audit event logged. I find that the Effective
Setting
> > > > > retain
> > > > > "no auditing" even the Local Setting is "Success". But when I
> > > > enable
> > > > > object

> > > > *access in Domain Controller Security Policy. The event log fill
up
> a
> > > lot
> > > > of
> > > > > entries with event id 560 & 562 and the user is administrator
(more
> > than
> > > a
> > > > thousand entries). However, nothing had been change or modify in
> the
> > > > files
> > > > > & folder directory from administrator account. Anyone encounter ?
> > Why
> > > > will
> > > > > it happens & how to disable these messages.
> > > > >
> > > > > Thanks in advance.
> > > > >
> > > > >
> > > >
> > > >
> > >
> > >
> >
> >
>
>*