

## Re: Record Layout of Windows Security Event log records ?.

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2004-02/0301.html>

---

**From:** Steen Schjellerup ([steenn\\_at\\_dk.ibm.com](mailto:steenn_at_dk.ibm.com))

**Date:** 02/27/04

Date: Fri, 27 Feb 2004 10:15:49 +0100

Hi Keith and Paul,

You have both been most helpfull, – thank you very much, it has been highly appreciated !.

I now have the record descriptions I need, – and I'll try the tool Paul found. Hopefully this will solve the problem with the interpretation of the accesses field also.

\*

Kind regards from  
Steen Schjellerup/Denmark.

"Paul Matear" <[paul@nospam.com](mailto:paul@nospam.com)> wrote in message  
news:OgBO0SN\$DHA.212@TK2MSFTNGP12.phx.gbl...

> *just found this reference which may help in finding the text strings*

>

>

> <http://groups.google.co.uk/groups?q=eventlog+accesses+565&hl=en&lr=&ie=UTF-8&oe=UTF-8&selm=bfop21%245pa%241%40FreeBSD.csie.NCTU.edu.tw&rnum=2>

>

> *best of luck!*

>

> *regards*

> *paul*

>

> "Paul Matear" <[paul@nospam.com](mailto:paul@nospam.com)> wrote in message

> news:Ubx%b.12185\$h44.1275619@stones.force9.net...

> > *Hi Steen*

> >

> > *I noticed 565 was missing, but as you said you'd already found that info*

> > *elsewhere. Info on all the security events you are interested in can be*

> > *found at <http://support.microsoft.com/default.aspx?scid=kb;en-us:299475>*

> > *and*

> > *its linked page*

> >

> > *From what I've seen of the Accesses field for event 565 and related 560,*

> *you*

> > *may have your work cut out trying to evaluate the values....*

microsoft.public.windows.server.security: Re: Record Layout of Windows Security Event log records ?.

> >

> > *normally things like WRITE\_OWNER and READ\_CONTROL are single bits within the*

> > *access mask (see*

> >

>

<http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/distsys/part2/dsgch12.asp>

> > *and*

> >

>

[http://msdn.microsoft.com/library/en-us/security/security/access\\_mask\\_format.asp](http://msdn.microsoft.com/library/en-us/security/security/access_mask_format.asp))

> > *but that doesn't seem to be the case here – also you need to know what the*

> > *textual values for the object specific bits are, and this will vary from*

> > *object to object. You may be able to determine the standard values by*

> > *trial*

> > *and error, but I'm guessing that there is an internal lookup table in the*

> > *event provider that gives the object specific values – possibly you might*

> > *hack this detail out....*

> >

> > *you seem quite comitted to programatically accessing this info from a low*

> > *level, but you might also consider using a tool such as LOGPARSER to extract*

> > *the events in a more useable fashion. LOGPARSER is a free tool from MS*

> > *designed for IIS logs but will also work against the EventLog. More info*

> > *on*

> > *this at [www.logparser.com](http://www.logparser.com) – you may find someone there (or at the*

> > *microsoft.public.inetsrv.iis newsgroup) that can give you some detail*

> > *on*

> > *how they implemented reading the event log records.*

> >

> > *hth*

> > *regards*

> > *paul*

> >

> > *"Steen Schjellerup" <[steenn@dk.ibm.com](mailto:steenn@dk.ibm.com)> wrote in message*

> > *news:%234D3E4E\$DHA.3220@TK2MSFTNGP10.phx.gbl...*

> > > *Hi Paul,*

> > > *Thank you very much for your reply.*

> > > *I'm only interested in Security event records with the event id of 565,*

> > > *624,*

> > > *628 and 632.*

> > > *The http address you gave me was nearly what I wanted. 2 things are*

> > > *missing*

> > > *though*

Re: Record Layout of Windows Security Event log records ?.

microsoft.public.windows.server.security: Re: Record Layout of Windows Security Event log records ?.

> > > 1). The layout of event id 565 is missing (not a big problem, – se the  
> > > bottom of this note)  
> > > 2). The translation mapping for the values which can be set for the  
> > > Accesses  
> > > field.  
> > > When I look in the raw record (after beeing transmitted to the  
> > > mainframe),  
> > > Everything looks like the descriptions I now have except for the  
> > > values  
> > > which is applied to the Accesses field.  
> > > What I see is something like Accesses %%7688 or there can be more than  
> > > just  
> > > one value after the Accesses field. There must be some kind of mapping  
> > > of  
> > > these values to a text because I have an example where the event  
> > > viewer  
> > > shows the Accesses field as "WRITE\_OWNER". Only problem I have is that  
> > > at  
> > > the moment I don't have that record at the mainframe, so I don't know  
> > > which  
> > > %%xxxx value corresponds to "WRITE\_OWNER". I also don't know if the  
> > > value  
> > > should be interpetet as a bit mask where one of the bits corresponds  
> > > to  
> > > "WRITE\_OWNER" or if the complete value tells me that it is  
> > > WRITE\_OWNER.  
> > > I  
> > > hope for the latter and also I think this is right because there can  
> > > be  
> > > many  
> > > %%xxxx values present after the Accesses field.  
> > >  
> > > The missing 565 record from your http address is not a big problem  
> > > because  
> > > I  
> > > have found it myself. I went to  
> > >  
> > >  
> > >  
> > > [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/  
> > > eventlogrecord\\_str.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/eventlogrecord_str.asp) and did a search for : event message 565, – the  
> > > first  
> > > entry from the search result (as I remember, – anyway there was only a  
> > > few)  
> > > got me to the record descriptions. Only in this case the 632 is  
> > > missing  
> > > so  
> > > your http address gave me the missing info. for that problem.  
> > >  
> > > Kind regards from  
> > > Steen Schjellerup/Denmark.

Re: Record Layout of Windows Security Event log records ?.

microsoft.public.windows.server.security: Re: Record Layout of Windows Security Event log records ?.

>>>  
>>>  
>>> *"Paul Matear" <paul@nospam.com> wrote in message*  
>>> *news:uBhVAK\$#DHA.4012@tk2msftngp13.phx.gbl...*  
>>>> *Hi Steen*  
>>>>  
>>>> *not sure I'm following what you are doing, but if you want to*  
*display*  
>> *the*  
>>>> *'friendly message' that you see in event viewer you may have a*  
> *problem.*  
>>> *Many*  
>>>> *event log messages are dynamically created when you view them in the*  
>>> *windows*  
>>>> *event viewer – the template text is contained in a supporting DLL*  
>> *specific*  
>>>> *for the source, and the eventlogrecord only contains the specific*  
> *values*  
>>> *for*  
>>>> *that record which are inserted as appropriate*  
>>>>  
>>>> *a list of registered event providers can be gathered from the*  
*registry*  
>>>> *(HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog)*  
>>>> *note that this list is specific for that machine – others may differ*  
>>>> *depending on what's installed*  
>>>>  
>>>> *for example security event messages are held in*  
>>>> *%systemroot%\system32\msaudite.dll*  
>>>>  
>>>  
>>  
>  
(HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\Secu  
>>>> *urity)*  
>>>> *if you have service packs applied there may be additional DLLs*  
> *specified*  
>>>>  
>>>> *the template text for common providers may also be gleaned from*  
> *various*  
>>>> *sources (as well as by extrapolating from the visible message in*  
*event*  
>>>> *viewer) such as*  
>>>> *<http://support.microsoft.com/default.aspx?scid=kb;en-us:174074>*  
>>>>  
>>>> *so you'd have to roll your own in that respect*  
>>>>  
>>>> *hth*  
>>>> *paul*  
>>>>  
>>>>

Re: Record Layout of Windows Security Event log records ?.

microsoft.public.windows.server.security: Re: Record Layout of Windows Security Event log records ?.

>>>>  
>>>> *"Steen Schjellerup" <steenn@dk.ibm.com> wrote in message*  
>>>> *news:uwT8qS7%23DHA.3184@TK2MSFTNGP09.phx.gbl...*  
>>>>> *Hello,*  
>>>>> *Thank you so fare for spending time on this issue.*  
>>>>> *Of course I have also spend further time on this and I have found*  
> *the*  
>>>>> *following:*  
>>>>> *I have found something which describes this to some point.*  
>>>>> *I went to*  
>>>>>  
>>>>>  
>>>  
>>  
>  
[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/  
eventlogrecord\\_str.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/eventlogrecord_str.asp) and did a search for : event message 565  
>>>>> *This gave me the layout of the 565 record, – simular is available*  
> *for*  
>>> *the*  
>>>>> *other events I have 2 problems though, a small and a bigger one*  
>>>>> *1) – the description is not to be included in any kind of program*  
as  
> *a*  
>>>>> *structure or typedef. The description is for humans to read. So*  
>>>> *something*  
>>>>> *which program languages likes would be nice (C, PL1, or simular).*  
> *Well*  
>> *I*  
>>>> *can*  
>>>>> *define an array of keywords myself which correspond to the ones*  
>>> *described*  
>>>>> *and hopefully I can write a program which will be able to find the*  
>>>>> *corresponding field values inside the record.*  
>>>>> *2) – The missing thing for me at the moment is the translation of*  
> *the*  
>>> *char*  
>>>>> *numeric values which are present after the Accesses keyword (the*  
> *ones*  
>>> *like*  
>>>>> *:*  
>>>>> *Accesses%%7688).*  
>>>>>  
>>>>> *Kind regards from*  
>>>>> *Steen Schjellerup/Denmark.*  
>>>>>  
>>>>>  
>>>>> *"Keith W. McCammon" <km@km.com> wrote in message*  
>>>>> *news:uHvHbx6#DHA.916@TK2MSFTNGP10.phx.gbl...*  
>>>>>> *I can't even find anything close. Let me check with someone on*  
> *this*

Re: Record Layout of Windows Security Event log records ?.

microsoft.public.windows.server.security: Re: Record Layout of Windows Security Event log records ?.

> > > *and*  
> > > > *get*  
> > > > > *back to you.*  
> > > > >  
> > > > >  
> > > > > *"Steen Schjellerup" <steenn@dk.ibm.com> wrote in message*  
> > > > > *news:Oun1yB5%23DHA.2804@tk2msftngp13.phx.gbl...*  
> > > > > > *Thanks for you comments, – but unfortunately it was not quite*  
> *what*  
> > *I*  
> > > > *need.*  
> > > > > > *I have found out that the all Windows Event log records have*  
*the*  
> > > *same*  
> > > > > *format. The format is the following:*  
> > > > > > *typedef struct \_EVENTLOGRECORD {*  
> > > > > > *DWORD Length;*  
> > > > > > *DWORD Reserved;*  
> > > > > > *DWORD RecordNumber;*  
> > > > > > *DWORD TimeGenerated;*  
> > > > > > *DWORD TimeWritten;*  
> > > > > > *DWORD EventID;*  
> > > > > > *WORD EventType;*  
> > > > > > *WORD NumStrings;*  
> > > > > > *WORD EventCategory;*  
> > > > > > *WORD ReservedFlags;*  
> > > > > > *DWORD ClosingRecordNumber;*  
> > > > > > *DWORD StringOffset;*  
> > > > > > *DWORD UserSidLength;*  
> > > > > > *DWORD UserSidOffset;*  
> > > > > > *DWORD DataLength;*  
> > > > > > *DWORD DataOffset;*  
> > > > > > *} EVENTLOGRECORD,*  
> > > > > > *\*PEVENTLOGRECORD;*  
> > > > > >  
> > > > > > > *The data reported from whatever component has been reporting*  
*to*  
> > *the*  
> > > > > *Event*  
> > > > > > > *log starts at "DataOffset" and has the length of "DataLength".*  
> > > > > > > *The records I'm interested in is the one reported as Security*  
> > *Events*  
> > > > > > > *(specifically event type 632, 624, 628 and 565).*  
> > > > > > > *Now what I need is the record layout of those Event types.*  
*This*  
> > *will*  
> > > > *be*  
> > > > > *a*  
> > > > > > > *seperate description of the complete Event log record namely*  
*the*  
> > > > > > > *structure/layout starting at "DataOffset".*

Re: Record Layout of Windows Security Event log records ?.

microsoft.public.windows.server.security: Re: Record Layout of Windows Security Event log records ?.

>>>>>> Also there are some equates which I need. For example for  
event  
>> type  
>>> 565  
>>>>>> "Directory Service Access" you can have the  
> accesses=WRITE\_OWNER.  
>>> This  
>>>>> is  
>>>>>> what is shown when you use the event viewer to look at the  
>>> records, –  
>>>>> but  
>>>>>> inside the actual record you only see Char Numeric values  
(like:  
>>>>>> Accesses%%7688), – so I need to know which value represents  
the  
>>>>>> WRITE\_OWNER  
>>>>>> access.  
>>>>>>> I guess Microsoft must have documented the record layouts for  
> each  
>>>>>>> event-id, – but I can't find it anywhere. I have been  
searching  
>>> around  
>>>>> in  
>>>>>>> the msdn Internet pages  
> (<http://msdn.microsoft.com/default.aspx> )  
>>>> that's  
>>>>>>> where I found the general layout for the Event Log records  
(the  
>>> common  
>>>>>>> prefix which are present in all Event Log records).  
>>>>>>> \*  
>>>>>>> I'm a manframe person, so I don't know who to contact for such  
>>>>>>> documentation  
>>>>>>> (I mean at the PC platform), – so if you can't guide me to the  
>> doc.  
>>>>>> maybe  
>>>>>>> you can help me get in contact with someone which can help me.  
>>>>>>> \*  
>>>>>>> Kind regards from  
>>>>>>> Steen Schjellerup/Denmark.  
>>>>>>>  
>>>>>>> "Keith W. McCammon" <km@km.com> wrote in message  
>>>>>>> news:#iAo\$Nv#DHA.2664@TK2MSFTNGP09.phx.gbl...  
>>>>>>>> Assuming you're talking about a database schema, this one is  
>>> handy:  
>>>>>>>>>  
>>>>>>>>> <http://www.winsyslog.com/common/en/faq/setup-with-mysql.asp>  
>>>>>>>>>  
>>>>>>>>>  
>>>>>>>>>  
>>>>>>>>> "Steen Schjellerup" <steenn@dk.ibm.com> wrote in message

Re: Record Layout of Windows Security Event log records ?.

